UNIVERSIDADE FEDERAL DE CAMPINA GRANDE
Centro de Engenharia Elétrica e Informática
Programa de Pós-Graduação em Engenharia Elétrica

Tese de Doutorado

Distribuição Quântica de Chaves com Modulação não Gaussiana: Protocolos, Desempenho e Segurança

Micael Andrade Dias

Campina Grande, Paraíba, Brasil

UNIVERSIDADE FEDERAL DE CAMPINA GRANDE
Centro de Engenharia Elétrica e Informática
Programa de Pós-Graduação em Engenharia Elétrica

Distribuição Quântica de Chaves com Modulação não Gaussiana: Protocolos, Desempenho e Segurança

Micael Andrade Dias

Tese de doutorado apresentada ao Programa de Pós-Graduação em Engenharia Elétrica da Universidade Federal de Campina Grande como parte dos requisitos necessários para obtenção do título de Doutor em Engenharia Elétrica.

Área de Concentração: Processamento da Informação
Linhas de Pesquisa: Eletrônica e Telecomunicações

Orientador: Francisco Marcos de Assis, Dr.

Campina Grande, Paraíba, Brasil

Agosto, 2023.

D541d Dias, Micael Andrade.
Distribuição quântica de chaves com modulação não gaussiana: protocolos, desempenho e segurança / Micael Andrade Dias. – Campina Grande, 2023.
198 f. : il. color.

Tese (Doutorado em Engenharia Elétrica) – Universidade Federal de Campina Grande, Centro de Engenharia Elétrica e Informática, 2023.
"Orientação: Prof. Dr. Francisco Marcos de Assis".
Referências.

1. Distribuição Quântica de Chave Secreta. 2. Modulação Discreta. 3. Convergência de Operadores. 4. Teoria da Informação Quântica. 5. Processamento da Informação. 6. Eletrônica. 7. Telecomunicações. I. Assis, Francisco Marcos de. II. Título.

CDU 621.391:530.145(043)

FICHA CATALOGRÁFICA ELABORADA PELA BIBLIOTECÁRIA SEVERINA SUELI DA SILVA OLIVEIRA CRB-15/225

Distribuição Quântica de Chaves com Modulação não Gaussiana: Protocolos, Desempenho e Segurança

MICAEL ANDRADE DIAS

TESE APROVADA EM 03/08/2023

FRANCISCO MARCOS DE ASSIS, Dr., UFCG
Orientador(a)

RAIMUNDO CARLOS SILVÉRIO FREIRE, Dr., UFCG
Examinador(a)

EDSON PORTO DA SILVA, Dr., UFCG
Examinador(a)

BARTOLOMEU FERREIRA UCHÔA FILHO, Dr., UFSC
Examinador(a)

PAULO ALEXANDRE CARREIRA MATEUS, Dr., IST
Examinador(a)

CAMPINA GRANDE - PB

MINISTÉRIO DA EDUCAÇÃO
UNIVERSIDADE FEDERAL DE CAMPINA GRANDE
POS-GRADUACAO EM ENGENHARIA ELETRICA
Rua Aprigio Veloso, 882, - Bairro Universitario, Campina Grande/PB, CEP 58429-900

REGISTRO DE PRESENÇA E ASSINATURAS

ATA DA DEFESA PARA CONCESSÃO DO GRAU DE DOUTOR EM CIÊNCIAS, NO DOMÍNIO DA ENGENHARIA ELÉTRICA, REALIZADA EM 03 DE AGOSTO DE 2023 **(Nº 364)**

CANDIDATO: **MICAEL ANDRADE DIAS**. COMISSÃO EXAMINADORA: RAIMUNDO CARLOS SILVÉRIO FREIRE, Dr., UFCG, Presidente da Comissão e Examinador Interno, FRANCISCO MARCOS DE ASSIS, Dr., UFCG, Orientador, EDSON PORTO DA SILVA, Dr., UFCG., Examinador Interno, BARTOLOMEU FERREIRA UCHÔA FILHO, Dr., UFSC, PAULO ALEXANDRE CARREIRA MATEUS, Dr., IST., Examinadores Externos. TÍTULO DA TESE: Distribuição Quântica de Chaves com Modulação não Gaussiana: Protocolos, Desempenho e Segurança. ÁREA DE CONCENTRAÇÃO: Processamento da Informação. HORA DE INÍCIO: **10h00** – LOCAL: **Sala Virtual, conforme Art. 5º da PORTARIA SEI Nº 01/PRPG/UFCG/GPR, DE 09 DE MAIO DE 2022**. Em sessão pública, após exposição de cerca de 45 minutos, o candidato foi arguido oralmente pelos membros da Comissão Examinadora, tendo demonstrado suficiência de conhecimento e capacidade de sistematização, no tema de sua tese, obtendo conceito APROVADO. Face à aprovação, declara o presidente da Comissão, achar-se o examinado, legalmente habilitado a receber o Grau de Doutor em Ciências, no domínio da Engenharia Elétrica, cabendo a Universidade Federal de Campina Grande, como de direito, providenciar a expedição do Diploma, a que o mesmo faz jus. Na forma regulamentar, foi lavrada a presente ata, que é assinada por mim, Filipe Emmanuel Porfírio Correia, e os membros da Comissão Examinadora presentes. Campina Grande, 3 de Agosto de 2023.

Filipe Emmanuel Porfírio Correia
Secretário

RAIMUNDO CARLOS SILVÉRIO FREIRE, Dr., UFCG
Presidente da Comissão e Examinador Interno

FRANCISCO MARCOS DE ASSIS, Dr., UFCG
Orientador

EDSON PORTO DA SILVA, Dr., UFCG
Examinador Interno

BARTOLOMEU FERREIRA UCHÔA FILHO, Dr., UFSC
Examinador Externo

PAULO ALEXANDRE CARREIRA MATEUS, Dr., IST
Examinador Externo

MICAEL ANDRADE DIAS
Candidato

2 - APROVAÇÃO

2.1. Segue a presente Ata de Defesa de Tese de Doutorado do candidato **MICAEL ANDRADE DIAS**, assinada eletronicamente pela Comissão Examinadora acima identificada.

2.2. No caso de examinadores externos que não possuam credenciamento de usuário externo ativo no SEI, para igual assinatura eletrônica, os examinadores internos signatários **certificam** que os examinadores externos acima identificados participaram da defesa da tese e tomaram conhecimento do teor deste documento.

Documento assinado eletronicamente por **RAIMUNDO CARLOS SILVERIO FREIRE**, **PROFESSOR 3 GRAU**, em 11/08/2023, às 10:32, conforme horário oficial de Brasília, com fundamento no art. 8º, caput, da Portaria SEI nº 002, de 25 de outubro de 2018.

Documento assinado eletronicamente por **FILIPE EMMANUEL PORFIRIO CORREIA**, **ASSISTENTE EM ADMINISTRACAO**, em 11/08/2023, às 10:46, conforme horário oficial de Brasília, com fundamento no art. 8º, caput, da Portaria SEI nº 002, de 25 de outubro de 2018.

Documento assinado eletronicamente por **Bartolomeu Ferreira Uchôa Filho**, **Usuário Externo**, em 11/08/2023, às 15:24, conforme horário oficial de Brasília, com fundamento no art. 8º, caput, da Portaria SEI nº 002, de 25 de outubro de 2018.

Documento assinado eletronicamente por **FRANCISCO MARCOS DE ASSIS**, **PROFESSOR 3 GRAU**, em 11/08/2023, às 16:11, conforme horário oficial de Brasília, com fundamento no art. 8º, caput, da Portaria SEI nº 002, de 25 de outubro de 2018.

Documento assinado eletronicamente por **EDSON PORTO DA SILVA**, **PROFESSOR(A) DO MAGISTERIO SUPERIOR**, em 14/08/2023, às 08:46, conforme horário oficial de Brasília, com fundamento no art. 8º, caput, da Portaria SEI nº 002, de 25 de outubro de 2018.

Documento assinado eletronicamente por **Micael Andrade Dias**, **Usuário Externo**, em 29/08/2023, às 10:31, conforme horário oficial de Brasília, com fundamento no art. 8º, caput, da Portaria SEI nº 002, de 25 de outubro de 2018.

A autenticidade deste documento pode ser conferida no site https://sei.ufcg.edu.br/autenticidade, informando o código verificador **3688224** e o código CRC **14DD062E**.

À minha esposa, Chris.

Agradecimentos

Agradeço a Deus por Sua bondade e misericórdia, que têm me acompanhado e possibilitado minha jornada acadêmica. Aos meus pais, Adiles e Marinaldo, que me ensinaram a importância dos estudos desde a infância. À minha esposa, Chris, que genuinamente nunca duvidou que eu pudesse alcançar meus objetivos.

Aos amigos com os quais tenho compartilhado a jornada acadêmica por um longo período: Felipe Pereira, desde o curso técnico integrado no CEFET, e Davi Juvêncio, desde a graduação em engenharia elétrica. Terei eterna gratidão pelo apoio, amizade e companheirismo que sempre estiveram presentes. Aos amigos que fiz fora da universidade, mas que sempre me apoiaram a enfrentar os desafios. Thyago, Amanda, Sebastião, Thayná, Barreto, Natã, Fernanda e tantos outros que não caberiam nessas páginas.

A todos os professores, mestres e doutores que contribuíram para minha formação. Em especial, ao meu orientador, Professor Francisco Marcos de Assis, com quem aprendi o valor da disciplina e da abstração, e que sempre foi generoso ao compartilhar conhecimento, experiência e conselhos. Também ao Professor Aércio Lima, que teve a generosidade de me ajudar no início dos estudos sobre óptica quântica.

A todos os amigos e colegas do iQuanta que tornaram a jornada mais leve e empolgante, compartilharam as dificuldades e alegrias, e com quem compartilho o interesse pela pesquisa e pela busca de perguntas mais curiosas. Em especial, à Milena, Andresso, Revson, Taciana e Thiciany.

Ao Programa de Pós-Graduação em Engenharia Elétrica (PPgEE - COPELE) da UFCG, pelo suporte administrativo. À CAPES, pelo suporte financeiro para o desenvolvimento desta tese.

"As coisas corajosas nas velhas histórias e canções, Sr. Frodo: aventuras, como eu costumava chamá-las. Eu costumava pensar que a gente maravilhosa das histórias saía para procurar porque queriam elas, porque elas eram emocionantes, e a vida era um pouquinho tediosa, uma espécie de esporte, poderíamos dizer. Mas esse não é o jeito das histórias que realmente importavam, nem das que ficam na lembrança. Normalmente parece que as pessoas simplesmente caíram dentro delas – os percursos delas foram traçados assim, como o senhor expressou. Mas acho que tiveram montes de oportunidades, assim como nós, de darem meia volta, só que não deram. E se tivessem dado, nós não iríamos saber, porque eles estariam esquecidos. Nós ouvimos falar dos que simplesmente foram em frente..."

Samwise Gamgee, O Senhor dos Anéis: as Duas Torres.

Resumo

Os protocolos de distribuição quântica de chave secreta (QKD) possibilitam que duas partes geograficamente distantes possam compartilhar e gerar sequências aleatórias e incondicionalmente seguras, uma tarefa para a qual não há contrapartida clássica e é possível pelas leis da mecânica quântica. Nas últimas décadas, tem sido de interesse o desenvolvimento e estudo dos protocolos definidos pela modulação não gaussiana (discreta) de estados coerentes (DM-CVQKD), os quais são compatíveis com dispositivos e arquiteturas usuais de comunicações ópticas, permitindo o compartilhamento de chaves em redes ópticas existentes. Nesta tese de doutorado, foram analisados os efeitos resultantes do uso de esquemas ótimos de modulação discreta no desempenho e segurança de protocolos DM-CVQKD. O primeiro resultado mostrado é que, sob a hipótese de ataques coletivos gaussianos, os esquemas de modulação que atingem a capacidade do canal gaussiano nas comunicações clássicas apresentam um comportamento análogo quando aplicados em protocolos DM-CVQKD. Em particular, foi identificada a necessidade de formatação probabilística para que um esquema de modulação discreta tenha desempenho próximo ao da modulação gaussiana, assim como a distribuição não uniforme de pontos no plano complexo para constelações com mais de 23^2 pontos. Voltando a atenção para a compatibilidade entre os protocolos QKD e a arquitetura de formatação probabilística de constelação, a susceptibilidade de geração de símbolos correlacionados foi discutida e um protocolo de reconciliação foi apresentado. Também foram desenvolvidos resultados relacionando a convergência de variáveis aleatórias e a convergência dos operadores de densidade induzidos pelas variáveis aleatórias. Dessa maneira, foi mostrado que o operador densidade que representa uma constelação converge fracamente para o estado térmico se a sequência de variáveis aleatórias que representa a constelação converge em distribuição para a distribuição normal. Como consequência, a "não gaussianidade" da constelação se aproxima de zero conforme a cardinalidade da constelação aumenta, assim como a diferença entre as taxas de chave do protocolo com modulação não gaussiana e seu equivalente gaussiano, sendo uma garantia de que o limitante inferior da taxa de chave secreta usualmente utilizado nas provas de segurança é justo se a constelação for grande o bastante. Por fim, foram apresentadas três proposições sobre a convergência (na norma do traço) das constelações de estados coerentes: um limitante para o erro de aproximação através da redução da dimensão do espaço de Hilbert (teste de energia), sobre a convergência do espectro de autovalores e autovetores, e a convergência da purificação da constelação de estados coerentes.

Palavras-Chaves: Distribuição Quântica de Chave Secreta. Modulação Discreta. Convergência de Operadores. Teoria da Informação Quântica.

Abstract

The quantum key distribution (QKD) protocols enable two geographically distant parties to share and generate random and unconditionally secure sequences, a task for which there is no classical counterpart and is made possible by the laws of quantum mechanics. In the recent decades, there has been interest in the development and study of protocols defined by discrete (non-Gaussian) modulation of coherent states (DM-CVQKD, Discrete Modulated Continuous-Variable QKD), which are compatible with usual optical communications devices and architectures, allowing key distribution over existing optical networks. In this doctoral thesis, the effects resulting from the use of optimal schemes of discrete modulation on the performance and security of DM-CVQKD protocols will be analyzed. The first result shown is that, under the assumption of Gaussian collective attacks, modulation schemes that achieve the capacity of the Gaussian channel in classical communications exhibit analogous behavior when applied in DM-CVQKD protocols. In particular, the need for probabilistic shaping was identified for a discrete modulation scheme to have performance close to Gaussian modulation, as well as the non-uniform distribution of points in the complex plane for constellations with more than 23^2 points. Shifting attention to the compatibility between QKD protocols and the probabilistic shaping architecture of the constellation, the susceptibility of generating correlated symbols was discussed, and a reconciliation protocol was presented. Results were also developed relating the convergence of random variables to the convergence of density operators induced by these random variables. It was shown that the density operator representing a constellation weakly converges to the thermal state if the sequence of random variables representing the constellation converges in distribution to the normal distribution. Consequently, the "non-Gaussianity" of the constellation approaches zero as the cardinality of the constellation increases, as well as the difference between the key rates of the non-Gaussian modulation protocol and its Gaussian counterpart, providing assurance that the lower bound commonly used in security proofs is fair if the constellation is large enough. Finally, three propositions are presented regarding the convergence (in trace norm) of coherent state constellations: a bound for the approximation error through dimension reduction of the Hilbert space (energy test), the convergence of the spectrum of eigenvalues and eigenvectors, and the convergence of the purification of the coherent state constellation.

Keywords: Quantum Key Distribution. Discrete Modulation. Operator Convergence. Quantum Information Theory.

Lista de Figuras

Lista de Tabelas

Lista de abreviaturas e siglas

APSK	*Amplitude-Phase Shift Keying*
AWGN	*Aditive White Gaussian Noise*
ASK	*Amplitude Shift Keying*
BCH	*Baker-Campbell-Hausdorff*
BER	*Bit Error Rate*
BHD	*Balanced Homodyne Detection*
BMD	*Bloch-Messiah Decomposition*
BPSK	*Binary Phase Shift Keying*
BS	*Beam Splitter*
BSC	*Binary Symetric Channel*
CPTP	*Completely Positive Trace Preserving*
CVQKD	*Continuous Variable Quantum Key Distribuction*
dFT	*de Finetti Theorem*
DM-CVQKD	*Discrete Modulated Continuous Variable Quantum Key Distribuction*
DVQKD	*Discrete Variable Quantum Key Distribuction*
DUD-CVQKD	*Discrete modulated Unidimensional Continuous Variable Quantum Key Distribuction*
EB	*Entangled Based*
ebit	*Entangled Bit*
EPR	*Einstein-Podolsky-Rosen*

FCW	*Função Característica de Wigner*
FEC	*Frame Error Correction*
GET	*Gaussian Extremality Theorem*
IR	*Information Reconciliation*
LDPC	*Low Density Parity-Check Codes*
LOCC	*Local Operations and Classical Communication*
MP	*Moore Penrose*
nG	*Non-Gaussian(ity)*
nGQRT	*Non-Gaussian Quantum Resource Theory*
OAPSK	*Optimal Amplitude-Phase Shift Keying*
P&M	*Prepare & Measure*
PAS	*Probabilistic Amplitude Shapping*
PCS	*Probabilistic Constellation Shapping*
POVM	*Positive Operato-Valued Measure*
PSK	*Phase Shift Keying*
QAM	*Quadrature Amplitude Modulation*
QBER	*Quantum Bit Error Rate*
QKD	*Quantum Key Distribution*
QPSK	*Quadrature Phase Shift Keying*
QRE	*Quantum Relative Entropy*
QRT	*Quantum Resource Theory*
qubit	*Quantum Bit*
RQF	*Resource Quantifying Function*
SEC	*Sliced Error Correction*
SKR	*Secret Key Rate*

SNPD	*Superconducting Nanowire Single-Photon Detector*
SNR	*Signal-to-Noise Rate*
SVD	*Singular Value Decomposition*
TPSK	*Ternary Phase Shift Keying*
TMSV	*Two-Mode Squeezed Vacuum*
UD-CVQKD	*Unidimensional Continuous Variable Quantum Key Distribuction*

Sumário

Parte I

Introdução

Capítulo 1

Introdução

Neste capítulo, será apresentada a motivação deste documento de tese, incluindo a revisão bibliográfica e a descrição do estado da arte, seguida pela organização do documento e a notação utilizada. Além disso, as contribuições destacam os pontos nos quais esta pesquisa colaborou com a comunidade científica.

1.1 Motivação

A distribuição quântica de chaves (QKD, do inglês: *Quantum Key Distribution*) surgiu da necessidade de duas partes legítimas, Alice e Bob, possuírem chaves secretas aleatórias disponíveis para uso em esquemas de criptografia que utilizam *one-time-pad*. Um protocolo QKD realiza a distribuição (ou geração) de chaves por meio da transmissão de estados quânticos através de um canal quântico inseguro e seu pós-processamento com o uso de um canal clássico autenticado. A espiã (Eva), por sua vez, tem controle total sobre o canal quântico e é capaz de observar toda a comunicação realizada pelo canal clássico autenticado. A segurança incondicional é possível pelas propriedades quânticas dos sistemas [1, 2, 3, 4], que tornam impossível que a espiã interfira na comunicação quântica de modo imperceptível [5, 6, 7, 8].

Os protocolos QKD têm sido classificados entre aqueles que se baseiam em sistemas quânticos de variáveis discretas, conhecidos como protocolos QKD de variáveis discretas (DVQKD, do inglês: *Discrete Variable* QKD) [9, 10, 11, 12], e os protocolos que manipulam sistemas quânticos de variáveis contínuas, chamados de protocolos QKD de variáveis contínuas (CVQKD, do inglês: *Continuous Variable* QKD) [13, 14, 15]. A primeira classe apresenta alta sensibilidade à temperatura dos fotodetectores, devendo operar a -120C° (InGaAs) ou a níveis criogênicos (SNSPD's) para que seja possível estabelecer comunicação em longas distâncias [16, 17]. Os protocolos da segunda classe,

por sua vez, podem ser realizados com equipamentos de comunicações ópticas usuais, mas exigem pós-processamento da chave com códigos corretores de erro e funções de quantização ótimas devido à modulação contínua aplicada [18, 19, 20, 21, 22].

A fim de evitar problemas de implementação e no pós-processamento, protocolos que aplicam modulação discreta em sistemas de variáveis contínuas (DM-CVQKD, do inglês: *Discrete Modulated* CVQKD) têm sido explorados como uma alternativa que mantém a compatibilidade com equipamentos usuais de comunicações ópticas e remove a exigência de realizar operações de quantização. Entretanto, a menor complexidade de implementação tem consequências no desempenho dos protocolos e aumenta a complexidade da análise de segurança, resultantes da modulação não gaussiana.

Uma das principais questões relativas ao desempenho de protocolos baseados em modulação discreta é que qualquer esquema de modulação não gaussiano é sub-ótimo na taxa de chave secreta gerada por estado transmitido, consequência do teorema da *extremalidade* gaussiana (GET, do inglês: *Gaussian Extremality Theorem*) [23, 24, 25]. Dessa maneira, encontrar esquemas de modulação (constelações) que aproximam o desempenho obtido por protocolos de modulação gaussiana surge como um importante ponto de investigação no estudo de protocolos DM-CVQKD. Esse problema é análogo ao investigado no contexto das comunicações clássicas em busca de constelações que "fecham a lacuna de capacidade" do canal de ruído aditivo gaussiano branco (AWGN, do inglês: *Aditive White Gaussian Noise*). Diversas técnicas têm sido aplicadas no contexto clássico, como as constelações unidimensionais investigadas por Wú e Verdu, cuja construção é baseada em polinômios de Hermite ou passeios aleatórios [26], e métodos de formatação geométrica e probabilística [27, 28] no caso bidimensional.

Contudo, as técnicas de formatação geométrica e probabilística de constelações realizam um processo de otimização a fim de ajustar os pontos de uma constelação padrão na direção de uma função de custo (a informação mútua) e não uma solução algébrica, como no caso das constelações de Gauss-Hermite que fazem o "casamento" de quadratura por meio dos polinômios (probabilísticos) de Hermite. No contexto dos protocolos QKD, poucas constelações com algum tipo de formatação têm sido utilizadas, principalmente no caso bidimensional. Destacamos o trabalho recente que analisa as constelações unidimensionais de [26] para protocolos CVQKD [29] e uma constelação do tipo QAM não equiprovável com distribuição binomial [30].

Com relação à análise de segurança dos protocolos DM-CVQKD, algumas questões podem ser destacadas partindo de um ponto principal: a análise de segurança dos protocolos CVQKD é realizada a partir do protocolo baseado em emaranhamento (EB, do inglês: *Entangled Based*) equivalente que, juntamente com a hipótese de que Eva

realiza ataques coletivos, permite que Alice e Bob admitam o compartilhamento de N cópias de um estado gaussiano bipartido a partir do qual é estimado o limite superior da informação acessível à espiã. No caso de protocolos DM-CVQKD, Alice e Bob aplicam modulação não gaussiana e o possível protocolo EB equivalente não utilizará estados bipartidos gaussianos.

A primeira consequência desse fato é que o desempenho estimado do protocolo também dependerá do modo de análise de segurança aplicado, e continuar usando a abordagem do protocolo EB assumindo estados gaussianos resulta na superestimação da informação acessível à espiã. Aqui, dois caminhos podem ser seguidos na investigação. O primeiro trata da proposição de técnicas alternativas para analisar a segurança dos protocolos DM-CVQKD que não partam da hipótese de que Alice e Bob compartilham estados gaussianos. A segunda é analisar o quanto a taxa de chave secreta é subestimada quando é utilizado um modelo de análise gaussiano em um esquema de transmissão com modulação não gaussiana, inclusive como essa quantidade se comporta quando a cardinalidade da constelação aumenta.

A segunda consequência se relaciona à equivalência entre ataques coletivos e coerentes. No primeiro, Eva interage individualmente com cada estado enviado, enquanto no último, todos os estados transmitidos por Alice são purificados por meio de um sistema quântico de referência controlado pela espiã. A análise de segurança para ataques coerentes se torna demasiadamente complicada e o caminho tomado é mostrar que ambos são equivalentes, ou que a chave final gerada pelo protocolo real considerando ataques coletivos é "próxima o suficiente" da chave gerada por um protocolo ideal que admite ataques arbitrários (com uma definição apropriada de norma para este caso).

O estudo da equivalência entre ataques coletivos e arbitrários para a segurança de protocolos QKD traz o sentido de segurança incondicional. Porém, seria possível elencar diversos pontos passíveis de verificação na proposta de um protocolo, desde questões práticas, como ruídos de modulação, detecção, térmicos, etc., até problemas teóricos como a composibilidade[1] [32, 33] de um protocolo e a análise da segurança da chave em comprimento finito [34, 35, 36]. A composibilidade, inclusive, é uma característica da segurança de um protocolo que deve ser contemplada quando se pensa na segurança *universal* de um protocolo QKD, isto é, que o resultado da execução desse protocolo (a chave secreta) é segura incondicionalmente, independentemente de como ela será aplicada. Uma formulação matemática de segurança universal de um protocolo foi proposta por Renner [33].

[1]Composibilidade é um princípio de projeto que considera as inter-relações entre componentes. Deste modo, um sistema destacadamente composível elabora componentes que possam ser escolhidos e montados em várias combinações, de modo a atender requisitos específicos do usuário [31].

A investigação dos aspectos teóricos e práticos da viabilidade e segurança dos protocolos CVQKD com modulações discretas torna possível a construção de redes seguras de comunicação utilizando infraestruturas compatíveis com as redes metropolitanas em uso. Este trabalho de tese propõe a investigação do desempenho de diversos esquemas de modulação levados ao limite da capacidade do canal de comunicação, assim como fornecer ferramentas para a análise de segurança compreendendo os aspectos não gaussianos dos esquemas de modulação.

Protocolos: Constelações e Segurança

Os protocolos de QKD de variáveis contínuas chamaram a atenção da comunidade de pesquisa em teoria da informação quântica com o protocolo GG02 [13, 14], baseado em modulação gaussiana de estados coerentes, e foram extensivamente examinados durante os anos subsequentes. De fato, esquemas de modulação contínua não gaussiana não têm sido explorados para aplicação em protocolos QKD, com exceção do protocolo baseado em mapas de Shannon-Kotel'nikov aplicados na preparação de estados, que além de não gaussiano é também não linear e funciona como um tipo de código corretor de erros analógicos, aumentando a relação sinal-ruído na recepção [37].

Apesar de, em 2002, um protocolo com um tipo de constelação com deslocamento em fase (PSK, do inglês: *Phase Shift Keying*) de dois estados coerentes ter sido apresentado [38], o estudo das modulações discretas aplicadas aos protocolos CVQKD ganhou força após a publicação do protocolo com constelação PSK binária (ou antipodal, BPSK, do inglês: *Binary* PSK) por Zhao *et al* [39]. Na Tabela 1, apresentamos um breve resumo dos protocolos DM-CVQKD e análises de segurança propostos desde então. Quando não especificado, a segurança do protocolo foi analisada para canais com ruído térmico (de excesso) resultante do modelo de ataque de clonagem por emaranhamento, ataques coletivos da espiã e limite assintótico da quantidade de estados transmitidos.

Dentre os protocolos desenvolvidos, podemos destacar alguns pontos. Um deles é que boa parte deles é baseada em constelações do tipo PSK, sendo diversos deles com quatro estados. Outro ponto é que poucos protocolos são propostos com alguma técnica de formatação de constelação para otimização da taxa de chave[2]. Destacamos as exceções dos protocolos apresentados por Djordjevic [40] e Kaur et al [41] – o primeiro realiza a otimização das amplitudes das subconstelações de um esquema com deslocamento em amplitude e fase (APK, do inglês: *Amplitude Phase Keying*), mantendo os estados equiprováveis, enquanto o segundo faz uso dos polinômios de

[2]Ressaltamos que alguns protocolos baseados em constelações do tipo PSK realizam a otimização do parâmetro de amplitude mas, como a geometria da constelação se mantém uniforme, não os contamos como geometricamente formatados.

Hermite, que alteram a geometria da constelação e as probabilidades de cada estado ser preparado.

Os protocolos apresentados na Tabela 1 foram analisados sob a hipótese de ataques coletivos (inclusive, com restrição para canais gaussianos), de modo que a análise de segurança contra ataques arbitrários de protocolos CVQKD com modulação discreta não se encontra no mesmo ponto de maturidade que os protocolos com modulação contínua gaussiana. Nestes, é possível encontrar na literatura resultados com limitantes para o parâmetro de segurança que estabelecem a equivalência entre ataques arbitrários e ataques coletivos [42, 43, 34, 35, 36].

Tabela 1 – Protocolos CVQKD com modulação discreta. Das abreviações, homódina (Hom.), heteródina (Het.), *Entangled Based* (EB), Prepara e Mede (P&M), reconciliação direta e reversa (R.D. e R.R., respectivamente).

Ano	Ref.	Mod.	Detec.	Tipo	Critérios para Segurança
2009	[39]	BPSK	Hom.	P&M	R.R.; detec. ideal.
2009	[8]	QPSK	Hom.	EB	R.R. ($\beta = 0.8$);
2010	[44]	m-PSK[a]	Het.	P&M	R.D./R.R.; canal sem ruídos; *postselection*; parâmetros otimizados.
2011	[45]	2,4,8-PSK	Hom/Het	EB	R.R.; *decoy states*.
2018	[46]	TPSK	Hom.	P&M	canal sem ruídos.
2018	[47]	m-PSK[b]	Het.	P&M	R.D./R.R.; espaço de Hilbert truncado.
2019	[40]	8-APSK	Het.	EB	R.R.; amplitudes otimizadas.
2019	[48]	QPSK	Het.	EB	R.R.; SDP.
2019	[49]	QPSK	Hom/Het	PM/EB	R.D./R.R.; Não usa o GET; *postselection*; espaço de Hilbert truncado.
2019	[50]	QPSK	Hom.	EB	R.R.; matrizes de cov. possíveis.
2020	[51]	QPSK	Hom.	EB	R.R.; amplificadores do tipo *quantum scissors*.
2021	[41]	m-APSK	Hom/Het	EB	R.R.; constelações de Gauss-Hermite; distância do traço como critério de continuidade.
2021	[30]	m-QAM	Het	EB	R.R.; constelações de Gauss-Hermite e Binomial; limitante inferior utilizando otimização semidefinida.
2021	[52]	m-PSK	Het.	PM	R.R.; Composibilidade e tamanho finito.
2023	[53][c]	m-QAM[b]	Het.	EB	R.R.; Composibilidade e tamanho finito.

[a] Os autores apresentam resultados para constelações com até 8 estados.
[b] Expressões desenvolvidas para m arbitrário mas os resultados apresentados foram para $m = 4$.
[c] Trabalho ainda não publicado em periódico.

1.2 Contribuições e Produção Científica

As contribuições desta tese de doutorado que a distingue de outros trabalhos estão listadas abaixo:

- Avaliação do desempenho de constelações ótimas no contexto clássico utilizadas na distribuição de chaves secretas. Foi identificado que as constelações que têm a propriedade de alcançar a capacidade do canal gaussiano nas comunicações clássicas tendem a ter desempenho semelhante quando aplicadas em protocolos CVQKD.
- Condições necessárias para a convergência dos operadores de densidade correspondentes a constelações com formatação geométrica e/ou probabilística para o estado térmico. O resultado afirma que se uma sequência de variáveis aleatórias converge em distribuição para a distribuição normal, a sequência de operadores de densidade da mistura induzida de estados coerentes converge para um estado térmico.
- Conexão entre a teoria de recursos quânticos não gaussianos e a análise de segurança de protocolos DM-CVQKD. Foi estabelecida uma medida de não gaussianidade para protocolos DM-CVQKD, a qual é função da medida de não gaussianidade do operador de densidade que representa a constelação.
- Proposta de protocolo de reconciliação que realiza a extração de *bits iid* e preserva a invariância do protocolo a permutações.
- Análise do ataque de clonagem por emaranhamento por meio da decomposição de Bloch-Messiah do estado compartilhado.

Os resultados dessas contribuições foram publicados em congressos nacionais e internacionais, bem como em periódicos da área, sendo eles:

- M. A. Dias e F. M. de Assis, "The impact of constellation cardinality on discrete unidimensional CVQKD protocols", Quantum Inf Process, vol. 20, nº 9, p. 284, set. 2021, doi: 10.1007/s11128-021-03222-w.
- M. A. Dias e F. M. de Assis, "Amplitude-Phase Modulated CVQKD Protocol", em Anais do XXXIX Simpósio Brasileiro de Telecomunicações e Processamento de Sinais, Sociedade Brasileira de Telecomunicações, 2021.
  doi: 10.14209/sbrt.2021.1570734220.

- M. A. Dias e F. M. Assis, "Evaluating the Eavesdropper Entropy via Bloch-Messiah Decomposition", em 2021 IEEE Conference on Communications and Network Security (CNS), Tempe, AZ, USA: IEEE, out. 2021, p. 1–6. doi: 10.1109/CNS53000.2021.9705021.

- M. Dias e F. M. de Assis, "Squeezed Vacuum State Approximation of Discrete Unidimensional Coherent State Constellations", em Anais de XXXVIII Simpósio Brasileiro de Telecomunicações e Processamento de Sinais, Sociedade Brasileira de Telecomunicações, 2020. doi: 10.14209/SBRT.2020.1570655315.

Trabalhos submetidos para publicação

- M. A. Dias e F. M. de Assis, "Distributional Transform Based Information Reconciliation". arXiv, 11 de maio de 2023, submetido para o *International Journal on Communication and Information Systems*.
Disponível em: http://arxiv.org/abs/2204.08891

- M. A. Dias e F. M. de Assis, "Converging State Distributions for Discrete Modulated CVQKD Protocols". arXiv, 10 de maio de 2023, submetido para a IEEE *Transactions on Communications*. Disponível em: http://arxiv.org/abs/2305.06484

1.3 Organização do Documento

O presente documento está dividido em sete capítulos. Neste capítulo de introdução, foram abordadas as motivações e os objetivos deste documento de tese. No Capítulo 2, será apresentada a estrutura geral de um protocolo QKD, os tipos de ataques de espionagem que estabelecem os níveis de segurança e ainda dois protocolos com modulação gaussiana que servirão como modelos de referência: o GG02 e o CVQKD unidimensional (UD-CVQKD, do inglês: *Unidimensional* CVQKD). O Capítulo 3 tratará do desempenho de protocolos CVQKD com modulação discreta considerando ataques coletivos, dando ênfase à formatação probabilística e geométrica das constelações em uma e duas dimensões. No Capítulo 4, será discutido como a arquitetura de um transmissor para constelações com formatação probabilística pode afetar a segurança incondicional do protocolo com modulação discreta, e no Capítulo 5, discutiremos a análise de segurança de protocolos DM-CVQKD do ponto de vista do ataque de clonagem por emaranhamento, propondo uma decomposição do ataque da espiã. O Capítulo 6 irá tratar do caráter não gaussiano das constelações utilizadas nos esquemas de modulação discreta, pela definição de uma medida de não gaussianidade do

protocolo e análise da convergência de operadores de densidade, resultando em condições para as quais o desempenho de um protocolo com modulação discreta converge para um protocolo com modulação gaussiana. Nos Apêndices A e B, constam os conceitos básicos em mecânica quântica, sistemas de variáveis contínuas e teoria da informação clássica e quântica, sendo a fundamentação teórica necessária para o desenvolvimento do trabalho.

Notação

Durante o trabalho será utilizada a notação de Dirac para mecânica quântica. Operadores lineares em sistemas quânticos são representados por letras maiúsculas, como $\hat{D}$, dos quais são diferenciado operadores de densidade por letras gregas, $\hat{\rho}$, em operadores canônicos de campo com letras minúsculas, $\hat{a}$. Vetores (matrizes) são representados por letras minúsculas (maiúsculas) em negrito, $\boldsymbol{x}$ ($\boldsymbol{M}$). Índices em estados/operados indicam a qual sistema o estado/operador pertence/atua e suas respectivas dimensões devem estar implícitas no contexto sempre que não mencionadas explicitamente. Sequências finitas serão denotadas com letras maiúsculas, X_N, sendo N seu comprimento, e seus elementos em letras minúsculas com índice indicando a posição na sequência, $X_N = x_1, \cdots, x_i, \cdots, x_N$.

Em específico, para um espaço de Hilbert $\mathcal{H}_A$, denotaremos por $\mathcal{B}(\mathcal{H}_A)$ o espaço dos operadores lineares limitados em $\mathcal{H}_A$ e $\mathcal{D}(\mathcal{H}_A)$ denotará o espaço dos operadores de densidade em $\mathcal{H}_A$. Sendo $\mathcal{L}(\mathcal{H}_A, \mathcal{H}_B) : \mathcal{L}(\mathcal{H}_A) \mapsto \mathcal{L}(\mathcal{H}_B)$ o espaço de todas as operações lineares levando elementos de $\mathcal{H}_A$ para $\mathcal{H}_B$, o subespaço $\mathcal{Q}(\mathcal{H}_A \to \mathcal{H}_B) \subset \mathcal{L}(\mathcal{H}_A, \mathcal{H}_B)$, ou apenas $\mathcal{Q}(A \to B)$, representa as operações quânticas completamente positivas e preservadoras do traço (CPTP, do inglês: *Completely Positive and Trace Preserving*), ou seja, canais quânticos, denotados por $\mathcal{N}_{A\to B} \in \mathcal{Q}(\mathcal{H}_A \to \mathcal{H}_B)$. Sempre que estiver claro no contexto, desconsideraremos a indicação dos sistemas de entrada e saída do canal, sendo $\mathcal{N} \in \mathcal{Q}$.

Parte II

Protocolos

Capítulo 2

Distribuição Quântica de Chave Secreta

Distribuir chaves secretas aleatórias por meio de sistemas quânticos é, em última instância, uma tarefa de geração de chaves (sequências binárias[1]) por meio do compartilhamento de estados quânticos transmitidos por Alice para Bob, as partes legítimas do protocolo. O que torna essa tarefa bem específica é que (i) a chave é aleatória, o que remove a obrigatoriedade de que a chave obtida ao final do protocolo seja idêntica à inicialmente transmitida, e (ii) a informação deve ser secreta. Logo, o protocolo deve se preocupar com o compartilhamento de informação lateral durante sua execução, uma vez que toda a comunicação estará sendo monitorada por uma espiã, Eva, a qual assumimos que é limitada apenas pela mecânica quântica.

Como apresentado no Capítulo 1, um protocolo QKD pode ser implementado utilizando diferentes plataformas. O primeiro protocolo QKD proposto, o BB84, utiliza fótons isolados como portadores de informação, que era codificada na polarização de cada fóton e compõe a classe de protocolos QKD com variáveis discretas (DVQKD). A segunda classe geral de protocolos utiliza estados de sistemas de variáveis contínuas (estados coerentes, comprimidos, térmicos, etc.) para transmitir informação que, por sua vez, é codificada pela modulação (contínua, em geral) da quadratura do estado, e cunha os protocolos de variáveis contínuas (CVQKD).

Neste capítulo, apresentaremos a estrutura padrão de um protocolo QKD, em específico para os de variáveis contínuas com modulação gaussiana simétrica e unidimensional, bem como os principais modelos de ataque de espionagem que podem ser realizados pela espiã.

[1]Aqui devemos ressaltar dois pontos importantes. (i) Apesar de que é teoricamente possível que as chaves sejam vetores de $\mathbb{R}^l$ (versão contínua do *one-time-pad* [54]), é conveniente que sejam sequências binárias por conta da compatibilidade com a informação a ser cifrada, esquemas de autenticação e códigos corretores de erros. (ii) Evitamos o termo "transmissão da informação" uma vez que as chaves são "geradas" durante a execução do protocolo QKD e não há seleção e transmissão de mensagens, conforme definida na teoria da informação.

2.1 O Protocolo Padrão

Um protocolo QKD tem como objetivo possibilitar que Alice e Bob consigam estabelecer uma chave aleatória que deve ser secreta a qualquer terceira parte que tente espionar a comunicação. A terceira parte, a adversária, é normalmente chamada de Eva, e admitimos que ela pode realizar ataques de espionagem que são limitados apenas pelas leis da mecânica quântica. O protocolo pode ser dividido em quatro etapas: a distribuição de estados que ocorre por meio de um canal quântico e a estimação de parâmetros, reconciliação das chaves (correção de erros) e amplificação de privacidade, que são realizadas com o uso de um canal clássico autenticado.

A primeira etapa de comunicação compreende a distribuição de estados quânticos. Alice gera uma sequência aleatória[2] X_L que deverá ser representada por L estados quânticos escolhidos de um conjunto não ortogonal de estados. Então, cada estado é preparado e transmitido para Bob por meio de um canal quântico que pode ser representado por um mapa completamente positivo e preservador do traço (do inglês, *Completely Positive Trace Preserving*). Bob, por sua vez, irá realizar a detecção dos estados afim de obter uma estimativa $Y_L = \hat{X}_L$ da sequência enviada por Alice. Devido aos ruídos do canal, inclusive as tentativas de espionagem, o resultado da primeira etapa de comunicação é o par de sequências correlacionadas X_L e Y_L. Essa estrutura do protocolo QKD é chamada de versão *Prepara e Mede* (P&M).

Outra forma de realizar a distribuição de estados quânticos é pelo compartilhamento de estados emaranhados entre Alice e Bob, chamado de protocolo baseado em emaranhamento (EB) equivalente ao P&M. A despeito da maior complexidade de implementação em relação ao protocolo P&M, o protocolo EB equivalente permite análises mais robustas de segurança. Nesta versão, Alice prepara L estados bipartidos de um sistema composto AB, representados no espaço de Hilbert $(\mathcal{H}_A \otimes \mathcal{H}_B)^{\otimes L}$. Alice mantém o primeiro modo[3], sobre o qual será realizada uma detecção projetiva, e o segundo modo é enviado para Bob pelo canal. Em [55], os autores mostram que sempre é possível associar um protocolo do tipo EB equivalente a um protocolo P&M. Para tal, considere como exemplo um protocolo P&M arbitrário em que Alice prepara estados puros não ortogonais de um conjunto $\{|\psi_k\rangle, p_k\}_{k=1}^{K}$ para

[2] $X_L = \{x_1, \cdots, x_L\}$, em que x_i é a i-ésima realização de uma variável aleatória $\mathcal{X}$. Para protocolos com modulação Gaussiana, $\mathcal{X} \sim \mathcal{N}(0, \tilde{V}_m)$ em geral, que serão descritos na Seção 2.3.

[3] No decorrer do trabalho, um "modo" se refere a um sistema físico representado por um oscilador harmônico quântico que corresponde a um modo de quantização do campo da onda eletromagnética. Para mais detalhes, vide o Apêndice A e as referências indicadas.

serem enviados para Bob. Equivalentemente, Alice poderia preparar o seguinte estado

$$|\psi\rangle_{AB} = \sum_{k=1}^{K} \sqrt{p_k}\, |k\rangle_A\, |\psi_k\rangle_B\,, \tag{2.1}$$

com $\{|k\rangle\}_{k=1}^{K}$ formando uma base ortonormal para $\mathcal{H}_A$, e aplicar uma medição projetiva com elementos $\{|1\rangle\langle 1|\,, \cdots, |K\rangle\langle K|\}$ no primeiro modo. Essa operação gera o resultado k com probabilidade p_k e projeta o segundo modo no estado $|\psi_k\rangle_B$. Para a espiã, os protocolos P&M e EB são indistinguíveis, e os dois protocolos são equivalentes em segurança. Logo, um protocolo do tipo P&M pode ter sua segurança analisada *substituindo a fonte* de estados quânticos, ou seja, obtendo um protocolo EB equivalente.

Na segunda etapa do protocolo, Alice e Bob utilizam $L' = L - l$ elementos de suas sequências X_L e Y_L escolhidos aleatoriamente para serem divulgados publicamente pelo canal clássico autenticado afim de estimar os parâmetros necessários para decidir se a etapa de comunicação quântica permite a geração de uma chave secreta. Para protocolos de variáveis contínuas, os parâmetros de interesse são a transmitância[4] e ruído de excesso do canal, os quais permitem a reconstrução da matriz de covariância. O objetivo aqui é obter um limitante superior da quantidade de informação obtida pela espiã durante a transmissão de estados quânticos. Os L' valores divulgados são então descartados, e Alice e Bob devem decidir se as sequências restantes X_l e Y_l, as *chaves brutas*, podem gerar uma chave segura ou se o protocolo deve ser abortado e reiniciado.

Uma vez que Alice e Bob decidem prosseguir para as próximas etapas, dois problemas precisam ser resolvidos: as sequências que compõem a chave bruta não são idênticas nem seguras. Elas não são idênticas devido ao ruído resultante do acoplamento do sistema principal com o sistema do ambiente, que também é o que as torna inseguras: a espiã exerce controle sobre o canal quântico principal realizando uma operação unitária universal em todos os sistemas transmitidos (cenário de ataques arbitrários) ou pelo acoplamento de um sistema auxiliar que interage individualmente com os estados transmitidos (ataques coletivos), de modo que o ruído observado na comunicação é induzido pelo acoplamento do sistema principal com o sistema auxiliar controlado pela espiã. A Seção 2.2 irá explorar o método de acoplamento realizado pela espiã e as estratégias utilizadas para obtenção de informação.

Na terceira etapa do protocolo QKD, reconciliação da informação, Alice e Bob utilizam comunicação por um canal clássico autenticado para executar um protocolo de

[4]Também chamado de transmissividade, é um parâmetro de atenuação inerente ao meio físico utilizado como canal de comunicação. Nesse trabalho de tese, será denotado pelo símbolo τ. Para fibras ópticas, a transmitância em função do comprimento d (em km) é dada pela relação $\tau = 10^{-0.01\cdot d}$.

correção de erros afim de concordarem com uma sequência binária U_l, resolvendo o primeiro problema da chave bruta. Quando a correção de erros toma Alice como referência, $U_l = X_l$, e Alice enviará informação lateral para Bob afim de que ele recupere X_l. Esse sentido de correção é chamado de *Reconciliação Direta*. A correção de erros também pode ser realizada com a *Reconciliação Reversa*, quando Bob é quem envia informação lateral para Alice afim de que ela recupere $Y_l = U_l$.

É importante ressaltar que, como a chave final deve ser uma sequência binária, ou seja, $U_l \in \{0,1\}^l$, os protocolos de variáveis contínuas devem realizar uma etapa de quantização da chave bruta antes da correção de erros [18, 22]. De modo geral, $X_l, Y_l \in \mathbb{R}^l$, então deve existir uma função $f : \mathbb{R}^l \to \{0,1\}^l$ de modo que, na reconciliação reversa, $U_l = f(Y_l)$. O uso da etapa de quantização nos protocolos CVQKD se torna então uma faca de dois gumes. Em teoria, é possível obter $b > 1$ bits por estado transmitido, resultando em chaves brutas de tamanho $l \cdot b$ para correção de erros. Mas, na prática, quanto mais bits são extraídos de cada estado, a correção de erros entre $f(X_l)$ e $f(Y_l)$ se torna mais difícil, exigindo que os códigos corretores de erro sejam extremamente eficientes.

A última etapa lida com a segurança da chave. Como descrito anteriormente, na distribuição quântica, a espiã tentará realizar algum ataque de espionagem afim de obter informação sobre os estados quânticos compartilhados por Alice e Bob, que podem decidir por abortar ou prosseguir com o protocolo QKD de acordo com os parâmetros estimados durante a segunda etapa. Uma vez estimado que a espiã não obteve informação suficiente para impedir o estabelecimento de uma chave segura, Alice e Bob prosseguem para corrigir os erros presentes em suas sequências e chegam a uma chave comum U_l. Como a espiã obteve informação pelo canal quântico e pelo canal clássico autenticado (e público), é preciso obter uma chave final S derivada de U_l que seja estatisticamente independente da informação da espiã, a chamada etapa de *amplificação de privacidade*. Normalmente, isso é feito com o uso de funções universais de *hashing* [32, 33] e compõe a última etapa do protocolo QKD.

2.2 Modelos de Ataques de Espionagem

Como apresentado, a execução do protocolo QKD ocorre em duas etapas: a comunicação quântica, na qual os estados são preparados, transmitidos e medidos, e a comunicação por um canal clássico autenticado, que resulta na chave secreta final. A ação da espiã será tentar obter informações sobre a chave compartilhada por Alice e Bob. Durante a comunicação pelo canal clássico (que é autenticado, mas não seguro!), Eva observará o conteúdo das mensagens trocadas (a informação lateral necessária para

a reconciliação das chaves, por exemplo) sem modificá-las.

No entanto, durante a comunicação quântica, a espiã pode interagir com os estados transmitidos por Alice, e o modelo do canal quântico está relacionado ao tipo de ataque realizado pela espiã. O resultado da interferência da espiã é a inevitável perturbação nos sistemas quânticos, que pode ser detectada por Alice e Bob durante a estimação de parâmetros. Em última instância, qualquer perda de informação para o sistema do ambiente durante a troca de estados pode (e será) entendida como informação obtida pela espiã, que controla a transmitância e o ruído de excesso do canal quântico.

Sendo o canal gaussiano um bom modelo para a transmissão de luz por fibras óticas [56] (um dos principais meios físicos para a implementação de protocolos QKD), é razoável considerar que Alice e Bob se comunicam por um canal gaussiano com ruído térmico aditivo, $\mathcal{E}^{th}_{\tau,\varepsilon}$, caracterizado pelas matrizes $\boldsymbol{T} = \sqrt{\tau}\boldsymbol{I}$ e $\boldsymbol{N} = (1-\tau)\varepsilon\boldsymbol{I}$, em que τ e ε são os parâmetros de transmitância e ruído térmico do canal, respectivamente. Em particular, o ruído térmico é definido como $\varepsilon = 2\bar{n} + 1$, sendo $\bar{n}$ o número médio de fótons térmicos. A ação do canal sobre um estado qualquer $\hat{\rho}$ com primeiro e segundo momentos estatísticos[5] $\bar{\boldsymbol{d}}$ e $\boldsymbol{\Gamma}$ será[6]

$$\bar{\boldsymbol{d}} \mapsto \boldsymbol{T}\bar{\boldsymbol{d}} = \sqrt{\tau}\bar{\boldsymbol{d}}, \tag{2.2}$$

$$\Gamma \mapsto \boldsymbol{T}\boldsymbol{\Gamma}\boldsymbol{T}^T + \boldsymbol{N} = \tau\boldsymbol{\Gamma} + (1-\tau)\varepsilon\boldsymbol{I}. \tag{2.3}$$

Fazendo a mudança de variável $2\bar{n} = \xi/(1-\tau)$, temos que $\boldsymbol{N} = [\xi + (1-\tau)]\boldsymbol{I}$, onde ξ é o "ruído de excesso" do canal, ou seja, a quantidade média de fótons adicionados ao modo devido ao acoplamento do sistema principal com o estado térmico do ambiente. Quando $\bar{n} = 0 \rightarrow \xi = 0$, o canal apenas atenua os estados sem adicionar ruído térmico (*pure loss channel*) [56, 57].

Eva pode então realizar um ataque físico, chamado de *máquina de clonagem por emaranhamento* [58], que emula $\mathcal{E}^{th}_{\tau,\varepsilon}$ acoplando o sistema principal com um estado de vácuo comprimido de dois modos (TMSV, do inglês: *Two-Mode Squeezed Vacuum*) $|\nu\rangle_{Ee}$ por meio de um divisor de feixe (BS, do inglês: *Beam Splitter*) com transmitância τ e escolhe a variância do ruído de quadratura de modo que $\nu = 1 + \xi/(1-\tau)$ [59], conforme apresentado na Figura 1.

A espiã detém uma das saídas do divisor de feixe que, juntamente com o segundo modo do estado TMSV (que não interagiu com o sistema de Alice), será detectada ou armazenada para medição posterior. A segunda saída do BS segue para Bob, que

[5] Para detalhes sobre os momentos estatísticos, consulte a Seção A.2 do Apêndice A.

[6] A transformação dos momentos estatísticos do estado realizada por $\mathcal{E}^{th}_{\tau,\varepsilon}$ é válida inclusive quando o canal atua sobre estados não gaussianos [56].

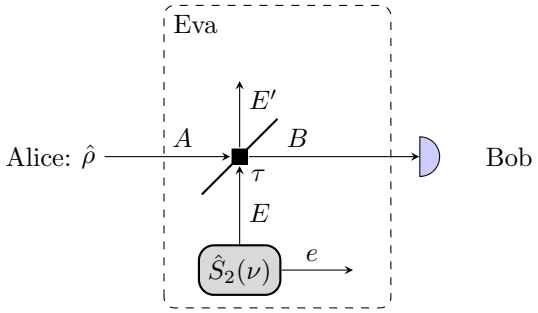


Figura 1 – Ataque de clonagem por emaranhamento.

"observará" o ruído térmico característico do canal. Durante a estimação de parâmetros, Alice e Bob devem estimar se o nível de ruído do canal indica a presença da espiã, comprometendo a continuidade do protocolo.

Tendo definido o modelo físico do ataque gaussiano realizado, podemos avançar na análise das diferentes maneiras pelas quais Eva pode proceder com a detecção.

2.2.1 Ataques Individuais

O primeiro nível de segurança supõe que Eva utiliza um estado auxiliar, normalmente chamado de *ancila*, para cada estado transmitido por Alice, e faz a detecção individualmente, conforme a Figura 2. A interação individual deve ser a mesma para todos os estados interceptados, e a medição não pode depender da informação clássica trocada por Alice e Bob, sendo realizada antes das etapas de reconciliação da informação e amplificação de privacidade. O resultado é que Eva obtém *informação clássica*, e as sequências aleatórias compartilhadas por Alice, Bob e Eva são classicamente correlacionadas.

Como Eva opera de maneira idêntica com cada estado interceptado, podemos dizer que o estado tripartido $|\Psi\rangle_{ABR}$ é um protótipo para cada rodada de comunicação, em que o sistema composto de referência[7] $R = Ee'$ é bipartido, de modo que

$$|\Psi\rangle_{ABR} = \mathbb{1}_A \otimes \hat{U}_{BE} \otimes \mathbb{1}_{e'} |\psi\rangle_{AB} |\nu\rangle_{Ee'} , \tag{2.4}$$

sendo $\hat{U}_{BE}$ o operador unitário que representa um divisor de feixe, $\mathbb{1}$ o operador identidade, e $|\psi\rangle_{AB}$ e $|\nu\rangle_{Ee'}$ os estados iniciais de Alice/Bob e Eva, respectivamente. As medições realizadas pelas três partes resultam nas sequências aleatórias X_L, Y_L e Z_L, que podem ser mapeadas no operador diagonal

$$\hat{\rho}_{ABE} = \sum_{X,Y,Z} p(X,Y,Z) |X\rangle\langle X| \otimes |Y\rangle\langle Y| \otimes |Z\rangle\langle Z| . \tag{2.5}$$

[7] Aqui, E e e' são os rótulos dos subsistemas que compõem o sistema composto R.

Logo, a informação obtida por Eva é a informação mútua clássica $I(X_L; Z_L)$, caso a reconciliação seja direta, ou $I(Y_L; Z_L)$, para a reconciliação reversa.

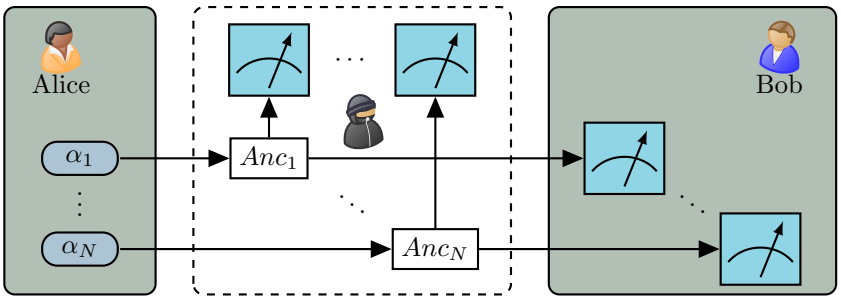


Figura 2 – Ataques Individuais.

2.2.2 Ataques Coletivos e Coerentes

Os ataques individuais, apesar de serem compatíveis com as tecnologias atuais, impõem fortes limitações nas capacidades de Eva: (i) interagir individualmente com cada estado e (ii) medir individualmente cada *ancila*. Um grande passo para tornar a segurança do protocolo QKD robusta é eliminar a restrição (ii), permitindo que Eva realize uma medição coletiva de todas as suas *ancilas*, estratégia classificada como *ataque coletivo*. Isso implica que Eva possui acesso a uma memória quântica, de modo que seus estados são armazenados e permite que a detecção seja realizada após a etapa de reconciliação. Nesse caso, Alice e Bob continuam compartilhando correlações clássicas pelas sequências aleatórias X_L e Y_L, mas Eva não deve realizar a detecção nesse ponto, mantendo um estado quântico $\hat{\rho}_E^{AB}$ correlacionado com as medições de Alice e Bob. As correlações CCQ (clássica-clássica-quântica) são representadas pelo estado

$$\hat{\rho}_{ABE} = \sum_{X,Y} p(X,Y) \, |A\rangle\langle A| \otimes |B\rangle\langle B| \otimes \hat{\rho}_E^{AB}, \tag{2.6}$$

e a informação obtida pela espiã é limitada pela quantidade de informação de Holevo, $\chi(A; E)$ ou $\chi(B; E)$ para reconciliação direta ou reversa, respectivamente, que informa a maior quantidade de informação acessível que é possível obter de um conjunto de estados quânticos por meio de medições apropriadas. Uma vez que Eva pode aguardar para observar a informação lateral compartilhada por Alice e Bob durante a etapa de reconciliação, ela pode utilizar essa informação para ajustar sua medição e obter POVMs (do inglês: *Positive Operator-Valued Measure*) ótimas e alcançar o limite de Holevo.

O próximo passo para uma análise de segurança sem restrições para a espiã consiste em remover a condição (i), permitindo que Eva interaja globalmente com todos os estados transmitidos, o que é conhecido como ataques coerentes ou arbitrários. Esse tipo de ataque

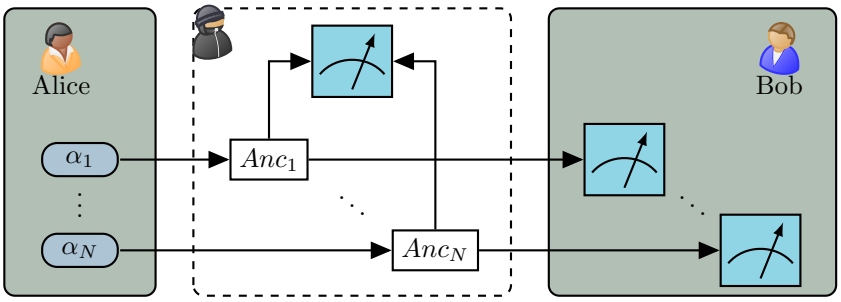


Figura 3 – Ataques Coletivos.

é realizado quando Eva possui um sistema de referência R que purifica todos os estados $\hat{\rho}_{AB}^{\otimes L}$ e cria correlações entre os estados transmitidos por Alice. A existência de tal sistema de referência é teoricamente possível, o que torna a análise de segurança difícil, de modo que a prática comum para obter segurança contra ataques arbitrários é provar que existe uma equivalência entre eles e os ataques coletivos, tema que será abordado rapidamente no Capítulo 5.

2.3 Protocolos Gaussianos

As Seções anteriores trataram de apresentar a finalidade de um protocolo QKD, as tarefas que o compõe, e como a espiã pode tentar interferir na comunicação, sem abordar com detalhes como os sistemas quânticos utilizados para transmitir informação, o tipo de modulação, detecção realizada por Bob, entre outros. Nesta Seção apresentaremos dois esquemas QKD baseados em modulação contínua Gaussiana que serão tratados como "pontos de referência" durante o desenvolvimento deste trabalho.

2.3.1 Modulação Simétrica

Tomaremos como ponto de partida os protocolos GG02 [13] e o *No-Switching protocol* [15]. Ambos aplicam modulação gaussiana nas quadraturas de estados coerentes, mas diferem no esquema de detecção realizado, sendo homódina no primeiro e heteródina no segundo, e nos ataques de espionagem considerados. Inicialmente, o protocolo GG02 foi provado incondicionalmente seguro contra ataques individuais, inclusive com demonstração experimental de seu funcionamento [14], e o *No-Switching protocol* para ataques do tipo *intercepta-e-reenvia*[8]. Posteriormente, Grosshans demonstrou em [60] a segurança do protocolo GG02 contra ataques coletivos, inclusive

[8]Nesse tipo de ataque, não abordado na seção anterior, Eva intercepta o estado coerente $|q_k + ip_k\rangle$, realiza a medição das duas quadraturas e obtém estimativas $\hat{q}_k$ e $\hat{p}_k$ das quadraturas originais. Então, ela prepara um estado coerente $|\hat{q}_k + i\hat{p}_k\rangle$ e o envia para Bob.

quando a detecção heteródina é aplicada. Abordaremos a discussão das provas de segurança incondicional contra ataques arbitrários no Capítulo 6.

Em sua versão P&M com detecção homódina, o protocolo é executado da seguinte maneira:

(i) Alice prepara L realizações de variáveis aleatórias i.i.d., $Q \sim P \sim \mathcal{N}(0, \tilde{V}_m)$, em que $\tilde{V}_m$ é chamada de variância de modulação, e forma as sequências aleatórias $Q_L = q_1, \cdots, q_L$ e $P_L = p_1, \cdots, p_L$, $Q_L, P_L \in \mathbb{R}^L$. Então, ela prepara L estados coerentes $|q_1 + ip_1\rangle, \cdots, |q_L + ip_L\rangle$ que são enviados para Bob pelo canal quântico caracterizado pela transmitância τ e ruído de excesso[9] ξ, ainda desconhecidos por ambos.

(ii) Bob, na recepção, irá realizar a detecção homódina, medindo uma das quadraturas de cada estado coerente enviado por Alice. A quadratura medida por Bob é escolha ao acaso de modo equiprovável. A sequência que denota os valores resultantes das medições realizadas por Bob é denotada por $Y_L = y_1, \cdots, y_L$. Bob informa a Alice sobre as quadraturas escolhidas afim de que ela descarte os valores discrepantes e mantenha os valores de Q_L ou P_L correspondentes à medição realizada para formar a sequência $X_L = x_1, \cdots, x_L$.

(iii) Alice e Bob escolhem aleatoriamente L' elementos das sequências X_L e Y_L para serem revelados afim de realizar a estimação de parâmetros do canal, sendo $L \lll L$ mantendo $l = L - L'$ valores de chave.

(iv) Com as sequências restantes, X_l e Y_l, Alice e Bob devem executar um protocolo de reconciliação da informação afim de concordarem em uma sequência binária $U \in \{0,1\}^{l \cdot b}$. Uma vez que os valores de X_l e Y_l são reais, deve haver um passo de quantização anterior à correção de erros extraindo b bits de cada elemento das sequências. Então, Alice e Bob realizam a etapa de correção de erros[10] das sequências binárias no sentido direto ou reverso para obterem uma sequência U_n comum a ambos.

[9] Ressaltamos que o ruído de excesso total ξ pode compreender ruídos oriundos de diversas fontes, como dos aparelhos de detecção (ruído eletrônico), moduladores de intensidade e fase, ruído térmico da fibra ótica, que também pode (e será) atrelado ao ataque de clonagem por emaranhamento realizado pela espiã [59].

[10] Em um protocolo de reconciliação da informação, a correção de erros compreende em Alice tornar sua sequência binária idêntica à de Bob (ou *vice-versa*). Como as chaves geradas devem ser aleatórias, não há uma etapa de codificação para transmissão dos elementos de chave, de modo que a "decodificação" (ou recuperação das sequências) é realizada através do paradigma de compressão de fontes correlacionadas com informação lateral [61, 19, 19, 62, 21]. De modo geral, Alice e Bob escolhem um código corretor de erros e Alice (ou Bob) envia a síndrome de sua sequência para Bob a fim de que ele corrija as diferenças entre as sequências através da decodificação utilizando a síndrome de Alice.

(v) Por fim, Alice e Bob precisam tornar a sequência U_n segura aplicando um protocolo de amplificação de privacidade. Este procedimento é o mesmo para qualquer protocolo QKD e é realizado pelo uso de famílias de funções *hashing*: Alice e Bob escolhem aleatoriamente uma função que mapeia a sequência U_n para uma sequência K cujo comprimento é calculado a partir dos parâmetros estimados durante a segunda etapa do protocolo.

Excetuando defeitos de equipamento, para o caso em que Bob realiza detecção heteródina, as sequências aleatórias X e Y ao final da etapa de comunicação quântica têm comprimento $2L$, não será realizada nenhuma etapa de compartilhamento de bases de medição e o restante do protocolo continuará identicamente ao descrito. Do ponto de vista de Alice, fazendo $\alpha = q + ip$, ela observa a mistura de estados

$$\hat{\rho} = \int_{\mathbb{C}} f(\alpha) \, |\alpha\rangle\langle\alpha| \, \mathrm{d}^2\alpha \, , \tag{2.7}$$

sendo $f(\alpha) = f_Q(q) f_P(p) = e^{-(q^2+p^2)/2\tilde{V}_m}/2\pi\tilde{V}_m$ a função de densidade de probabilidade conjunta de P e Q e $\mathrm{d}^2\alpha = \mathrm{d}(q)\,\mathrm{d}(p)$. O número médio de fótons emitidos por estado é dado por

$$\langle\hat{n}\rangle = \mathrm{tr}(\hat{n}\hat{\rho}) = \int_{\mathbb{C}} f(\alpha) \, \mathrm{tr}(\hat{a}^\dagger\hat{a} \, |\alpha\rangle\langle\alpha|) \, \mathrm{d}^2\alpha \, , \tag{2.8}$$

$$= \int_{\mathbb{C}} f_Q(q) f_P(p)(q^2 + p^2) \, \mathrm{d}q \, \mathrm{d}p \, , \tag{2.9}$$

$$= 2\tilde{V}_m = \bar{m}. \tag{2.10}$$

que é a energia média da modulação, e a variância dos operadores de quadratura será

$$V(\hat{q}) = \mathrm{tr}(\hat{q}^2\rho) = 4\tilde{V}_m + 1 = 2\bar{m} + 1 = V(\hat{p}). \tag{2.11}$$

Realizando o procedimento de substituição de fonte, é possível obter um protocolo EB equivalente com Alice tendo posse de um estado TMSV. Alice realiza uma medição heteródina no primeiro modo e então o segundo modo é preparado condicionalmente em um estado coerente [14]. O modo projetado em um estado coerente é então enviado para Bob pelo canal quântico e o restante do protocolo segue identicamente ao esquema P&M. A equivalência é devida ao fato de que um observador externo ao laboratório de Alice não consegue distinguir se Alice iniciou um protocolo baseado em emaranhamento ou do tipo prepara e mede.

Então, partindo do protocolo EB equivalente, o estado compartilhado por Alice e Bob sendo gaussiano pode ser descrito pelos momentos estatísticos e tem matriz de covariância

$$\boldsymbol{\Sigma}_{AB} = \begin{pmatrix} V\boldsymbol{I} & \sqrt{V^2-1}\boldsymbol{Z} \\ \sqrt{V^2-1}\boldsymbol{Z} & V\boldsymbol{I} \end{pmatrix}, \tag{2.12}$$

sendo $V = 2\bar{m} + 1$ de modo que aplicando o traço no primeiro modo, o modo restante corresponde estatisticamente à mistura da Equação (2.7) observada por Bob no protocolo P&M. Uma vez que consideramos o ataque de clonagem por emaranhamento, descrito na Seção 5.1, Eva prepara um estado TMSV $|\nu\rangle\, Ee'$, de modo que o estado do sistema composto $ABEe'$ é $\boldsymbol{\Sigma}ABEe' = \boldsymbol{\Sigma}_{AB} \oplus \boldsymbol{\Sigma}_{Ee'}$ e a espiã substitui o canal entre Alice e Bob por um divisor de feixe de transmitância τ. A transformação simplética dos quatro modos envolvidos é dada pela matriz de transformação do divisor de feixe aumentada

$$\boldsymbol{BS}_{BE} = \begin{pmatrix} \boldsymbol{I} & \boldsymbol{0} & \boldsymbol{0} & \boldsymbol{0} \\ \boldsymbol{0} & t\boldsymbol{I} & r\boldsymbol{I} & \boldsymbol{0} \\ \boldsymbol{0} & -r\boldsymbol{I} & t\boldsymbol{I} & \boldsymbol{0} \\ \boldsymbol{0} & \boldsymbol{0} & \boldsymbol{0} & \boldsymbol{I} \end{pmatrix}, \tag{2.13}$$

em que $t = \sqrt{\tau}$ e $r = \sqrt{1-\tau}$. Após o ataque de clonagem, a matriz de covariância total do sistema é transformada para $\boldsymbol{BS}BE\boldsymbol{\Sigma}ABEe'\boldsymbol{BS}_{BE}^{T}$ de modo que o estado final compartilhado por Alice e Bob terá a matriz de covariância

$$\boldsymbol{\Sigma}'_{AB} = \begin{pmatrix} V\boldsymbol{I}_2 & \sqrt{\tau}\sqrt{V^2-1}\boldsymbol{Z} \\ \sqrt{\tau}\sqrt{V^2-1}\boldsymbol{Z} & [\tau V + (1-\tau)\nu]\boldsymbol{I}_2 \end{pmatrix} \tag{2.14}$$

que, Eva escolhendo a variância do ruído de quadratura (ruído térmico) para $\nu = 1 + \xi/(1-\tau)$, a matriz de covariância final do estado compartilhado por Alice e Bob após o canal quântico será

$$\boldsymbol{\Sigma}'_{AB} = \begin{pmatrix} V\boldsymbol{I}_2 & \sqrt{\tau}\sqrt{V^2-1}\boldsymbol{Z} \\ \sqrt{\tau}\sqrt{V^2-1}\boldsymbol{Z} & [\tau(V-1)+1+\xi]\boldsymbol{I}_2 \end{pmatrix} = \begin{pmatrix} \boldsymbol{\Sigma}'_A & \boldsymbol{\Sigma}'_C \\ \boldsymbol{\Sigma}'^{T}_C & \boldsymbol{\Sigma}'_B \end{pmatrix}. \tag{2.15}$$

que é a matriz esperada quando o modo B é transmitido por um canal térmico sem a presença de uma espiã[11]. Caso Bob realize detecção homódina, sua matriz de covariância é transformada em

$$\boldsymbol{\Sigma}'_{A|B} = \boldsymbol{\Sigma}'_A - \boldsymbol{\Sigma}'_C(\boldsymbol{\Pi}_*\boldsymbol{\Sigma}'_B\boldsymbol{\Pi}_*)^{-1}\boldsymbol{\Sigma}'^{T}_C \tag{2.16}$$

sendo $\boldsymbol{\Pi}_* = \boldsymbol{\Pi}_q = \mathrm{diag}(1,0)$ caso a quadratura q seja medida e $\boldsymbol{\Pi}_* = \boldsymbol{\Pi}_p = \mathrm{diag}(0,1)$ para a quadratura p. Para o caso em que Bob realiza detecção heteródina,

$$\boldsymbol{\Sigma}'_{A|B} = \boldsymbol{\Sigma}'_A - \boldsymbol{\Sigma}'_C(\Sigma'_B + \boldsymbol{I})^{-1}\boldsymbol{\Sigma}'^{T}_C. \tag{2.17}$$

Para estratégias de ataques coletivos, Eva realiza o mesmo tipo de ataque físico para todos os estados transmitidos por Alice e o estado da Equação (2.15) pode ser tomado como um "protótipo" para análise de segurança. Alice e Bob irão reconciliar suas

[11] Para tal, basta fazer as matrizes aumentadas para o canal térmico, $\boldsymbol{T} = \boldsymbol{I} \oplus \sqrt{\tau}\boldsymbol{I}$ e $\boldsymbol{N} = \boldsymbol{0} \oplus (1-\tau)\varepsilon\boldsymbol{I}$ ($\boldsymbol{0}$ é a matriz nula de dimensão 2×2) e escrever o ruído térmico na forma $\varepsilon = 1 + \xi/(1-\tau)$.

sequências e obter até $I(X;Y)$ bits de informação por pulso e devem, na amplificação de privacidade, remover a informação da espiã que é dada pelo limitante de Holevo $\chi(E,B)$, no caso de reconciliação reversa. A quantidade de Holevo pode ser calculada através da matriz de covariância $\mathbf{\Sigma}'_{Ee'}$ do estado de Eva após o ataque de emaranhamento ou, admitindo de modo geral que Eva detém uma purificação do estado de Alice e Bob, temos que $S(E) = S(AB)$, $S(E|B) = S(A|B)$ e, logo, $\chi(B,E) = S(E) - S(E|B) = S(AB) - S(A|B)$. Por fim, a taxa de chave segura contra ataques coletivos ao final do protocolo será

$$K = \beta I(A;B) - \chi(E,B), \tag{2.18}$$

em que $\beta \in \{0,1\}$ representa a eficiência do protocolo de reconciliação.

2.3.2 Modulação Unidimensional

A principal ideia do protocolo CVQKD com modulação unidimensional (UD-CVQKD) [63] é realizar a modulação gaussiana em uma única quadratura (sem perda de generalidade, a quadratura q). Isso implica que deve ser estabelecida uma relação de equilíbrio entre o desempenho do protocolo e a complexidade de implementação: reduzir a modulação a uma única quadratura compromete seu desempenho (em relação ao GG02), mas simplifica a modulação e a detecção dos estados (modulador de intensidade e detecção homódina).

No protocolo (P&M), Alice prepara estados coerentes em que as amplitudes reais q são realizações de uma variável aleatória gaussiana $Q \sim \mathcal{N}(0, \tilde{V}_m)$. Isso induz, pela função de densidade de probabilidade gaussiana $f_Q(q) = e^{-q^2/2\tilde{V}_m}/\sqrt{2\pi\tilde{V}_m}$, a seguinte mistura contínua de estados

$$\hat{\rho}_G = \int_{-\infty}^{\infty} f_Q(q)\, |q\rangle\langle q|\, \mathrm{d}q\,, \tag{2.19}$$

que apresenta energia média $\langle \hat{n} \rangle = \tilde{V}_m$. Para as quadraturas, temos que $\Delta p = 1$ e $\Delta q = \sqrt{V_m + 1}$, sendo $V_m = 4\tilde{V}_m$. Os estados preparados são transmitidos para Bob por um canal quântico que realizará a detecção homódina em cada estado recebido.

O protocolo baseado em emaranhamento (EB) equivalente consiste em Alice realizar uma operação de compressão em um modo com parâmetro $r = -\log\sqrt{V}$ no segundo modo de um estado TMSV, cuja matriz de covariância é transformada para

$$\mathbf{\Gamma}_{AB} = \begin{pmatrix} V & 0 & \sqrt{V(V^2-1)} & 0 \\ 0 & V & 0 & -\sqrt{\frac{V^2-1}{V}} \\ \sqrt{V(V^2-1)} & 0 & V^2 & 0 \\ 0 & -\sqrt{\frac{V^2-1}{V}} & 0 & 1 \end{pmatrix}, \tag{2.20}$$

sendo $V^2 = V_m + 1$. Alice pode então preparar condicionalmente um estado coerente no segundo modo de 2.20 aplicando uma medição homódina no primeiro modo, analogamente ao protocolo GG02. Os estados coerentes preparados condicionalmente são enviados pelo canal[12] com transmitância τ e ruído de excesso[13] $\varepsilon = 1 + \tau\xi/(1-\tau)$, e a matriz de covariância do estado após o canal (e consequentemente, os ataques realizados pela espiã) será

$$\mathbf{\Gamma}'_{AB} = \begin{pmatrix} V & 0 & \sqrt{\tau}\sqrt{V(V^2-1)} & 0 \\ 0 & V & 0 & -\sqrt{\tau}\sqrt{\frac{V^2-1}{V}} \\ \sqrt{\tau}\sqrt{V(V^2-1)} & 0 & 1+\tau(V_m+\xi) & 0 \\ 0 & -\sqrt{\tau}\sqrt{\frac{V^2-1}{V}} & 0 & 1+\tau\xi \end{pmatrix}, \tag{2.21}$$

$$= \begin{pmatrix} \mathbf{\Gamma}'_A & \mathbf{\Gamma}'_C \\ \mathbf{\Gamma}'^T_C & \mathbf{\Gamma}'_B \end{pmatrix}. \tag{2.22}$$

Na recepção, Bob aplica a detecção homódina na quadratura q, que condiciona o estado, resultando na matriz de covariância $\mathbf{\Gamma}'_{A|B}$ obtida pela medição parcial descrita pela Equação (2.16). A taxa de chave secreta para ataques coletivos, assintoticamente, e considerando o sentido reverso de reconciliação $R_{cont} = I(A;B) - \chi(E,B)$ é então calculada a partir das matrizes $\mathbf{\Gamma}'_{AB}$ e $\mathbf{\Gamma}'_{A|B}$, sendo a informação mútua

$$I(A;B) = \frac{1}{2}\log\left(1 + \frac{\tau V_m}{1+\tau\xi}\right). \tag{2.23}$$

A taxa de chave secreta contra ataques coletivos, considerando o sentido reverso de reconciliação, será dada pela expressão

$$K = \beta I(A;B) - \chi(E,B), \tag{2.24}$$

em que as quantidades, a informação mútua (clássica) e a quantidade de Holevo, podem ser calculadas pelas matrizes de covariância $\mathbf{\Gamma}'AB$ e $\mathbf{\Gamma}A|B'$, assumindo que Eva detém uma purificação do estado compartilhado por Alice e Bob.

Distribuição Quântica de Chave Secreta

Nesse capítulo, foi apresentado como duas partes geograficamente separadas, Alice e Bob, podem fazer uso de sistemas quânticos para gerar chaves secretas, tarefa

[12] No escopo deste trabalho, assumimos que o canal é simétrico em seus invariantes simpléticos, apresentando a mesma transmissividade e ruído em ambas as quadraturas. Na análise realizada em [63], foi analisado o caso assimétrico em que Alice e Bob devem realizar medições na quadratura não modulada para estimar também os parâmetros para a quadratura p.

[13] A fim de manter a notação em [63], no protocolo UD, foi adotada uma substituição diferente da utilizada no protocolo GG02.

realizada pelos protocolos QKD, com foco no uso de sistemas quânticos de variáveis contínuas. Também foram abordadas as principais categorias de ataque de espionagem que a adversária, Eva, pode realizar a fim de obter informações sobre as sequências compartilhadas por Alice e Bob, e como um protocolo CVQKD com modulação gaussiana pode ser analisado pela matriz de covariância dos estados quânticos bipartidos que são utilizados na versão baseada em emaranhamento. No próximo capítulo, serão explorados os esquemas de modulação não gaussiana obtidos pela utilização de constelações de estados coerentes, como as taxas de chave secreta podem ser calculadas a partir do protocolo P&M para o canal sem ruídos e como o desempenho do protocolo é afetado pela utilização de um esquema não gaussiano de modulação.

Capítulo 3

Protocolos CVQKD com Modulação Discreta

No Capítulo 2, foi apresentado o modelo padrão de um protocolo do tipo QKD, que pode ser implementado com base em sistemas quânticos de variáveis contínuas (CVQKD) ou discretas (DVQKD), e foi descrita a estrutura básica da análise dos protocolos baseados em modulação gaussiana simétrica (Seção 2.3.1) e unidimensional (Seção 2.3.2). Dentre as etapas de um protocolo, a transmissão de estados e a reconciliação de informação para protocolos DV e CV são implementadas de maneiras distintas[1]. Para a transmissão de estados quânticos, é bem claro: protocolos DVQKD utilizam um conjunto finito de estados quânticos de sistemas de variáveis discretas para codificar as sequências binárias, enquanto os protocolos CVQKD utilizam modulação contínua (gaussiana) das quadraturas de estados de sistemas contínuos. Não só a preparação, mas também a detecção de estados é bastante diferente, uma vez que protocolos DVQKD normalmente utilizam a polarização do fóton como portadora da informação [9] e aplicam detecção de fótons isolados, que é extremamente sensível aos ruídos. Esquemas CVQKD, por sua vez, aplicam detecção homódina/heteródina das quadraturas de estados coerentes, por exemplo [64, 59], sendo compatíveis com tecnologias de comunicações ópticas disponíveis comercialmente.

Quanto à reconciliação da informação, protocolos DVQKD são mais simples, pois não exigem a etapa de quantização necessária para mapear em sequências binárias os valores contínuos resultantes da detecção de estados coerentes, presente nos protocolos CVQKD, como abordado na Seção 2.1. Na última década, as pesquisas em QKD têm se voltado para uma solução híbrida, com o objetivo de manter as melhores características

[1]Destacamos que a etapa de estimação de parâmetros também ocorre de maneira distinta entre protocolos DVQKD e CVQKD, mas é possível desconsiderar qualquer diferença de complexidade de implementação.

de ambas as classes de protocolos por meio da aplicação de modulação discreta em sistemas quânticos de variáveis contínuas (DM-CVQKD). Com esses protocolos, não há necessidade de uma conversão contínua-discreta, e a compatibilidade com os dispositivos de comunicações ópticas atuais é mantida usando estados coerentes. Essa passagem da modulação contínua (analógica) para a modulação discreta (digital) é um processo já experimentado em sistemas de comunicação clássicos, nos quais a modulação Gaussiana, que corresponde ao comportamento estatístico de um canal de ruído gaussiano e atinge a capacidade do canal, é aproximada por esquemas de sinalização digital.

Neste capítulo, serão apresentados alguns protocolos DM-CVQKD e seus desempenhos (taxa de chave secreta) sob a hipótese de ataques coletivos. Na Seção 3.1, serão revisados alguns conceitos de modulação discreta nos sistemas clássicos de comunicação, inclusive as condições para que uma constelação alcance a capacidade do canal gaussiano. Na Seção 3.2, serão apresentados os resultados de taxas de chave secreta relativas à utilização de famílias de constelações unidimensionais com formatação probabilística e/ou geométrica para definir um protocolo CVQKD. Inicialmente, os resultados consideram um canal atenuante sem ruído, com a finalidade de identificar se as constelações que apresentam bom desempenho no paradigma clássico mantêm o mesmo comportamento quando aplicadas ao paradigma de distribuição de chaves. Os resultados serão então estendidos na Seção 3.3, utilizando os limitantes inferiores para a taxa de chave secreta desenvolvidos em [30] que permitem o cálculo da taxa de chave secreta para canais gaussianos, comparando o desempenho de constelações do tipo m-QAM obtidas pelo produto cartesiano das constelações unidimensionais.

3.1 Modulação Discreta nas Comunicações Clássicas

O canal de alfabeto contínuo com ruído aditivo gaussiano ocupa uma posição de destaque no estudo da transmissão da informação, pois fornece um modelo preciso para diversos meios físicos, como a conexão entre satélites e a fibra óptica [65, 56]. O canal AWGN é discreto no tempo, com saída $y_i = x_i + z_i$ no tempo i, sendo x_i a entrada do canal e z_i uma realização da variável aleatória $Z \sim \mathcal{N}(0, N)$ independente de x_i. Caso o canal apresente variância de ruído nula ou os sinais de entrada sejam irrestritos em potência, o canal AWGN terá capacidade infinita, exceto por uma probabilidade de erro negligível.

Em geral, o ruído tem variância não nula e os sinais de entrada do canal são restritos à energia média P. Sendo $X = \{x_i\}$ o alfabeto na entrada do canal, temos

$$\sum_{i=1}^{M} p_i \mathcal{E}_i \leq P, \tag{3.1}$$

sendo $\mathcal{E}_i = |x_i|^2$ a energia do i-ésimo sinal associado à probabilidade p_i. A capacidade (informacional) do canal gaussiano submetido à restrição de potência P é

$$C_G = \max_{E[\mathcal{E}]\leq P} I(X;Y) = \frac{1}{2}\log\left(1+\frac{P}{N}\right), \tag{3.2}$$

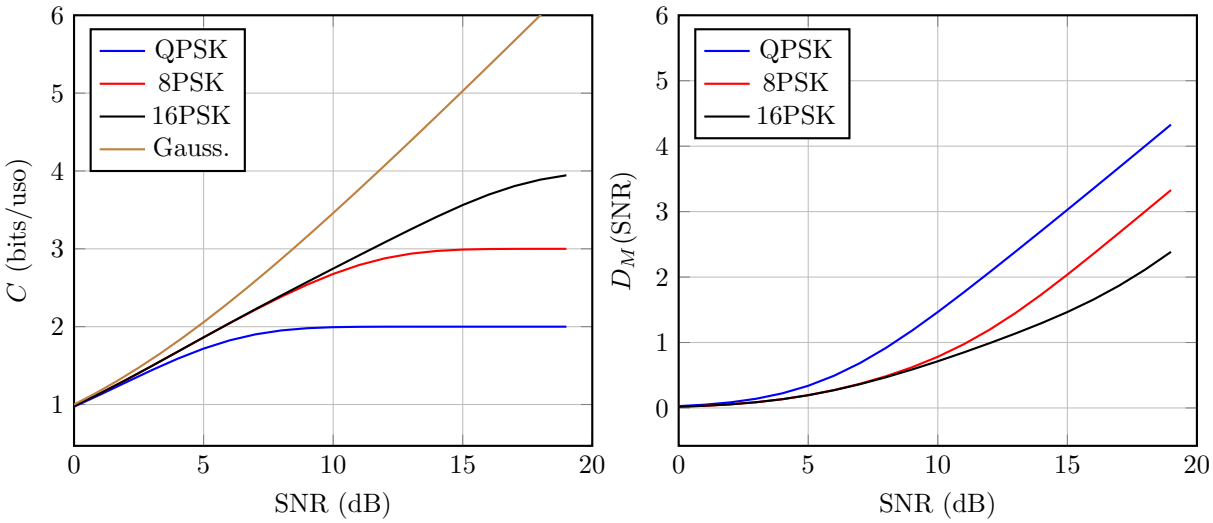
sendo a maximização no espaço dos conjuntos dos sinais de entrada submetidos à restrição de potência, cujo máximo é obtido quando X consiste em um alfabeto contínuo com distribuição $X \sim \mathcal{N}(0,P)$. Isso implica que o esquema de modulação gaussiana "alcança" a capacidade do canal AWGN, pois seu comportamento probabilístico "combina" com o do modelo do canal. A capacidade C é então função apenas da quantidade P/N, a razão sinal-ruído (snr, do inglês: *Signal to Noise Ratio*). É possível ainda assumir que a entrada do canal pode assumir valores complexos e que o canal é caracterizado pelo ruído aditivo simétrico. Então, N_i terá distribuição gaussiana circular (partes reais e imaginárias independentes e com variância $N/2$). Mantendo a restrição de energia, a capacidade será

$$C_{G^*} = \log\left(1+\frac{P}{N}\right). \tag{3.3}$$

Entretanto, a modulação gaussiana não é compatível com os sistemas modernos de transmissão de informação. Além disso, a transmissão de sinais digitais exige que os sinais transmitidos representem sequências binárias que deverão ser recuperadas na recepção. Por isso, esquemas de *modulação digital* mapeiam, por meio de sinalizações discretas, as sequências de símbolos m-ários (normalmente $m = 2$) em um conjunto finito de sinais a serem transmitidos pelo canal de comunicação. Esse conjunto finito de sinais é chamado de *constelação* e invariavelmente tem desempenho inferior à modulação gaussiana, como resultado do uso de modulação não gaussiana.

Dentre os diversos esquemas de modulação digital, destacam-se as constelações tradicionalmente usadas com sinais modulados em amplitude (ASK), em fase (PSK) e a modulação em amplitude e quadratura (QAM). Nessas modulações, a informação é codificada na amplitude ou fase (ou ambas) dos sinais transmitidos, e a quantidade de informação transmitida depende não apenas da snr, mas também da cardinalidade da constelação. A capacidade informacional alcançada será, então, a informação mútua entre o alfabeto de entrada (discreto real ou complexo) e a saída do canal (contínua, real ou complexa), que operacionalmente representa a maior taxa de bits transmitidos por uso do canal de maneira confiável para o canal com ruído gaussiano aditivo. Considerando o caso complexo, a probabilidade de saída y do canal com variância $N/2$ em cada quadratura condicionada à entrada x_1 será

$$p(y|x_1) = \frac{1}{\pi N} e^{-\frac{|y-x_i|^2}{N}}. \tag{3.4}$$



(a) Capacidade informacional. (b) Lacuna de capacidade.

Figura 4 – Capacidade do canal com ruído aditivo gaussiano branco complexo e capacidade para modulações discretas tipo PSK.

A Figura 4a apresenta a capacidade informacional de um canal AWGN com entradas complexas em função da snr. A curva superior indica o limite imposto pelo canal, alcançado pela modulação gaussiana, e as demais curvas apresentam a capacidade alcançada por constelações m-PSK com $m = \{4, 8, 16\}$. É possível notar uma diferença expressiva de desempenho entre a modulação gaussiana e os esquemas de modulação digital. Por exemplo, o canal impõe que, para transmitir dois bits de informação, é preciso ter uma snrum pouco menor que 5 dB, enquanto a snrdeve ser de pelo menos 8 dB para que seja possível transmitir dois bits de informação utilizando um esquema de modulação QPSK ($m = 4$). A essa diferença entre os valores de snrnecessários para transmitir a mesma quantidade de informação com modulação gaussiana e um esquema de modulação m-ário não gaussiano damos o nome de "lacuna de formatação" [27]. Analogamente, podemos definir a "lacuna de capacidade" como a diferença entre a capacidade informacional da modulação gaussiana e não gaussiana [26] para o mesmo valor de snr. Defina $C(\mathsf{snr})$ como a capacidade do canal gaussiano e $C_{m,*}(\mathsf{snr})$ como a capacidade da constelação $(*)$ com m sinais. A lacuna de capacidade é definida como $D_{m,*}(\mathsf{snr}) = C(\mathsf{snr}) - C_{m,*}(\mathsf{snr})$. Os respectivos valores de $D_{m,*}$ para constelações PSK são apresentados na Figura 4b.

As constelações retangulares, como QAM, com sinais equiprováveis e uniformemente distribuídos, apresentam desempenho próximo à capacidade do canal em regiões de baixa snr, mas saturam em $\log(m)$, sendo m a cardinalidade da constelação. Nas regiões de alta snr, entretanto, o valor da lacuna de formatação é assintoticamente igual a $\pi e/6 \approx 1.53$ dB, consequência do formato da constelação. O mesmo fenômeno acontece para a modulação

unidimensional ASK que, no limite,

$$\lim_{\mathsf{snr}\to\infty}\lim_{m\to\infty} D_M(\mathsf{snr}) = \frac{1}{2}\log\Big(\frac{\pi e}{6}\Big) \approx 0.25\,\text{bits}, \tag{3.5}$$

que resulta em uma "perda" efetiva de snrde aproximadamente 1.53 dB ao usar o esquema ASK [26].

É então razoável questionar se é possível que um esquema de modulação discreta aproxime arbitrariamente a capacidade do canal gaussiano, o que é chamado de "fechar" ou "preencher" a lacuna de capacidade[2] e qual é a forma dessa constelação. A fim de resolver esse problema, surgem os métodos de *formatação de constelação*. As constelações QAM apresentam uma "geometria" uniforme (subconjuntos de $\mathbb{Z}^2 - (\frac{1}{2}, \frac{1}{2})$ marcam os "lugares" dos sinais no espaço bidimensional) e são equiprováveis. Portanto, a formatação geométrica (probabilística) irá modificar a geometria (probabilidade) de cada sinal, de modo que ela se torne mais parecida com uma modulação gaussiana. Em termos assintóticos, para cardinalidades grandes das constelações, os dois métodos conseguem fechar a lacuna de capacidade, aproveitando de forma mais eficiente o canal gaussiano.

3.1.1 Condição de Alcance da Capacidade do Canal AWGN

Nesta seção, revisaremos alguns resultados importantes sobre distribuições que aproximam a capacidade do canal. A seguir, usamos algumas definições e resultados de [26, 66] para estabelecer as noções básicas que serão exploradas na configuração do QKD.

Definição 3.1 (Lacuna de Capacidade do Canal AWGN [26])**.** *Seja* $C(\mathsf{snr}) = \frac{1}{2}\log(1+\mathsf{snr})$ *a capacidade de um AWGNC e* $C_m(\mathsf{snr}) = \sup I(X; \sqrt{\mathsf{snr}}X + N)$ *a capacidade do canal AWGN restrita a uma constelação de m pontos. O supremo é assumido sobre todas as distribuições de probabilidade de X cujos suportes satisfazem* $|supp(P_X)| \leq m$*. A lacuna mínima de capacidade de uma constelação de m pontos é definida como*

$$D_m(\mathsf{snr}) = C(\mathsf{snr}) - C_m(\mathsf{snr}). \tag{3.6}$$

Encontrar as distribuições ótimas para uma constelação de pontos m não é uma tarefa trivial[3] e o intervalo mínimo de capacidade de (3.6) pode não ser alcançado para

[2]Em termos operacionais, podemos usar os termos "lacuna de capacidade" e "lacuna de formatação" de forma intercambiável.

[3]Na verdade, em [26], os autores enfatizam que ainda não são conhecidas constelações de pontos m ótimas em $\mathbb{R}^2$ com valores arbitrários de m, embora tenham mostrado constelações assintoticamente boas para o caso unidimensional.

um m arbitrário. Seja X_n uma variável aleatória sob as mesmas condições da Definição 3.1 e denote por $C_{X_n}(\mathsf{snr}) = I(X_n; \sqrt{\mathsf{snr}}X_n + N)$ a máxima taxa de informação para o canal AWGN com símbolos de entrada extraídos de X_n. Em seguida, definimos a lacuna de capacidade relativa à constelação não ótima X_n, quando possível, como

$$D_{X_n}(\mathsf{snr}) = C(\mathsf{snr}) - C_{X_n}(\mathsf{snr}) \geq D_m(\mathsf{snr}). \tag{3.7}$$

Para lidar com a convergência das medidas de probabilidade, vamos adotar uma abordagem teórica de medidas. Sejam (X, d) e (Y, ρ) espaços métricos separáveis com σ-álgebras de Borel $\mathcal{X}$ e $\mathcal{Y}$, respectivamente[4]. Um canal sem memória é definido como uma medida de probabilidade (um *kernel*) $\nu(\cdot, \cdot) : X \times \mathcal{Y} \to [0, 1]$, onde para cada $x \in X$, $\nu(x, \cdot)$ é uma medida de probabilidade (probabilidade condicional $P_{Y|X}(F|x)$) e para cada $B \in \mathcal{Y}$, $\nu(\cdot, B)$ é mensurável.

Exemplo 3.2. *Considere $X = Y = \mathbb{R}$ e o canal AWGN com $N_0 = 1$. Então,*

$$\nu(x, B) = \frac{1}{\sqrt{2\pi}} \int_B e^{-(y-x)^2/2} dy. \tag{3.8}$$

Definição 3.3 (Divergência)**.** *Dado um espaço mensurável comum $(\Omega, \mathcal{A})$ e duas medidas de probabilidade P e M nele, a divergência $D(P||M)$ é definida como*

$$D(P||M) = \sup_{\mathcal{R} \in P_{\mathcal{A}}} \sum_{R \in \mathcal{R}} P(R) \log \frac{P(R)}{M(R)}, \tag{3.9}$$

onde $P_{\mathcal{A}}$ é a coleção de $\mathcal{A}$ partições mensuráveis finitas de Ω.

Definição 3.4 (Capacidade do Canal)**.** *A capacidade do canal C sob restrição (c, Γ) pode ser definida como*

$$C = \sup_{\substack{Q \in \mathcal{Q} \\ \int c(x)Q(dx) \leq \Gamma}} D(PQ||Q \times M_Q) \tag{3.10}$$

onde $\mathcal{Q}$ é a coleção de medidas de probabilidade em $\mathcal{X}$.

Hipótese 3.5 (Continuidade Fraca de Canais)**.** *Para cada $x \in X$, o kernel $\nu(\cdot, \cdot)$ é fracamente contínuo em x, ou seja, se $x_n \to x$ ($(x_n)_{n \in \mathbb{N}} \subset X$) então $\nu(x_n, \cdot) \to \nu(x, \cdot)$.*

Teorema 3.6 ([66])**.** *Considere uma sequência $(Q_n)_{n \in \mathbb{N}}$ de medidas de probabilidade sobre $\mathcal{X}$ as quais convergem para a medida de probabilidade Q. Se a Hipótese 3.5 se mantém, então $PQ_n \Rightarrow PQ$. Ainda mais,*

$$\liminf_{n \to \infty} D(PQ_n||Q_n \times M_{Q_n}) \geq D(PQ||Q \times M_Q). \tag{3.11}$$

[4]O desenvolvimento com a teoria da medida foi retirado de [66]. Mais detalhes também podem ser encontrados em [67].

Teorema 3.7 (Convergência de medidas de probabilidade e Capacidade do canal [66])**.** *Suponha que as condições da Teorema 3.6 são satisfeitas e que Q é um medida de probabilidade com $C = D(PQ||Q \times M_Q)$ e $\int c(x)D(\mathrm{d}x) \leq \Gamma$. Então, qualquer sequência $(Q_n)_{n\in\mathbb{N}}$ de medidas de probabilidade em que $Q_n \Rightarrow Q$ e obedece à restrição de energia apresenta a seguinte propriedade*

$$D(PQ_n||Q_n \times M_{Q_n}) \to C. \tag{3.12}$$

Pela equivalência entre convergência fraca de medidas de probabilidade e convergência em distribuição das respectivas sequências de variáveis aleatórias (ou seja, se $X_n \xrightarrow{\mathcal{D}} X$ então $P_{X_n} \Rightarrow P_X$ [68]), é consequência do Teorema 3.7 que pela Definição 3.1, se $X_n \xrightarrow{\mathcal{D}} X$ então $D_{X_n}(\mathsf{snr}) \to 0$.

3.1.2 Constelações Unidimensionais

No que se segue, serão revisadas rapidamente quatro famílias de constelações unidimensionais que alcançam a capacidade do canal AWGN em diferentes regimes de relação sinal-ruído [26], as quais são definidas de forma genérica por um conjunto $\mathcal{A}$ de m amplitudes reais e uma distribuição de probabilidade $\mathcal{P}$ que representa a probabilidade de cada sinal em $\mathcal{A}$ ser preparado (transmitido).

Definição 3.8 (Equilattice [69])**.** *Seja E_m um conjunto de m pontos igualmente espaçado na reta real*

$$E_m = \begin{cases} \{2i\Delta_m\} : i = \frac{1-m}{2}, \cdots, 0, \cdots, \frac{m-1}{2} \ (m \ odd) \\ \{(2i+1)\Delta_m\} : i = -\frac{m}{2}, \cdots, 0, \cdots, \frac{m-1}{2} \ (m \ even) \end{cases}. \tag{3.13}$$

A constelação Equilattice (EQ) é definida pelo conjunto de amplitudes $\mathcal{A}_{EQ} = E_m$ equiprováveis, $\mathcal{P}_{EQ} = U_m$.

Definição 3.9 (Quantile [70])**.** *Considere os $m+1$ pontos da reta real a seguir,*

$$-\infty = \alpha_1 < \alpha_2 < \cdots \alpha_m < \alpha_{m+1} = \infty, \tag{3.14}$$

de modo que

$$\frac{1}{\sqrt{2\pi}} \int_{\alpha_i}^{\alpha_{i+1}} e^{-\frac{x^2}{2}} \, \mathrm{d}x = \frac{1}{m}. \tag{3.15}$$

Seja $\{x_i\}$ o conjunto de m centroides das partições equiprováveis definidas por α_i, obtidos da seguinte maneira:

$$x_i = \frac{m}{\sqrt{2\pi}} \int_{\alpha_i}^{\alpha_{i+1}} x e^{-\frac{x^2}{2}} \, \mathrm{d}x \, . \tag{3.16}$$

Então, a constelação Quantile (QU) é definida pelas amplitudes $\mathcal{A}_{QU} = \{x_i\}$ da Equação (3.16) com distribuição uniforme $\mathcal{P}_{QU} = U_m$.

Definição 3.10 (Gauss quadrature [26]). *Para uma função densidade gaussiana padrão* $p_X(x) = \frac{1}{\sqrt{2\pi}} e^{-x^2/2}$ *o m-ésimo polinômio de Hermite,* H_m*, é dado por*

$$H_m(x) = \frac{(-1)^m}{p_X(x)} \frac{\mathrm{d}^m p_X(x)}{\mathrm{d}x^m}. \tag{3.17}$$

As m raízes $\{x_{i,m}\}$ *de* H_m *em conjunto com o conjunto de pesos*

$$w_{i,m} = \frac{(m-1)!}{m H_{m-1}^2(x_{i,m})},$$

que forma uma distribuição de probabilidades legítima ($w_{i,m} > 0$ *and* $\sum_i w_{i,m} = 1$*), também conhecida como quadratura de Gauss (GQ). Então, a constelação de quadratura gaussiana (Gauss Quadrature, GQ) é composta pelo conjunto de amplitudes* $\mathcal{A}_{GQ} = \{x_{i,m}\}$ *e a distribuição de probabilidades* $\mathcal{P}_{QU} = \{w_{i,m}\}$*.*

Definição 3.11 (Random walk [26]). *Para a caminhada aleatória normalizada*

$$X_N = \frac{1}{\sqrt{m-1}} \sum_{k=1}^{m-1} Z_k, \tag{3.18}$$

em que Z_k *são i.i.d. em* $\{1, -1\}$*, é possível verificar a seguinte convergência em distribuição*

$$X_m \overset{D}{=} \frac{2}{\sqrt{m-1}} \left(B_N - \frac{m-1}{2} \right), \tag{3.19}$$

sendo $B_m \sim \mathrm{Binomial}(m-1, 1/2)$*. Então, a constelação "caminhada aleatória" (RW) de m pontos é definida pela variável aleatória* X_m*, ou seja, o conjunto de amplitudes* $\mathcal{A}_{RW} = \left\{ (2i - m + 1/\sqrt{m-1}) \right\}_{i=0}^{m-1}$ *e a distribuição de probabilidades* $\mathcal{P}_{RW} = \mathrm{Bin}(m-1, 1/2)$*.*

No contexto dos protocolos CVQKD baseados em estados coerentes, essas quatro famílias de constelações resultam em diferentes *ensembles* induzidos pelas combinações de amplitudes e distribuições de probabilidade. Para qualquer formato de constelação, a variância de modulação $\tilde{V}_m$ (energia média da constelação) é igual ao número médio $\bar{n}$ de fótons do *ensembles*: para uma determinada mistura de estados $\hat{\rho} = \sum_{i=1}^{m} p_i \left|\alpha_i\right\rangle\!\left\langle\alpha_i\right|$, em que o conjunto de amplitudes $\{\alpha_i\}$ e probabilidades $\{p_i\}$ são dados por qualquer constelação definida acima, temos que

$$\tilde{V}_m = \sum_{i=1}^{m} p_i \alpha_i^2 = \sum_{i=1}^{m} p_i \left\langle \alpha_i | \hat{a}^\dagger \hat{a} | \alpha_i \right\rangle = \mathrm{tr}(\hat{n}\hat{\rho}) = \langle \hat{n} \rangle \tag{3.20}$$

que é a mesma identidade encontrada para o protocolo UD-CVQKD P&M apresentado na Seção 2.3.2. Todas as constelações devem ser normalizadas corretamente para corresponder à energia média necessária da constelação. De maneira geral, as

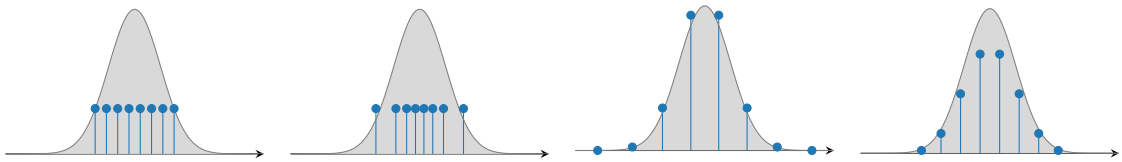


Figura 5 – Constelações unidimensionais com $m = 8$. Da esquerda para a direita: EQ, QU, GQ, RW.

constelações podem ser classificadas tanto pela sua formatação geométrica quanto probabilística, ou seja, pela distribuição dos pontos na reta real, definindo as amplitudes dos estados e as probabilidades atribuídas a cada amplitude [27]. Nesses termos, QU apresenta formatação geométrica, RW formatação probabilística, GQ é formatada de maneira geométrica e probabilística, e EQ é uniforme (símbolos equidistantes e equiprováveis).

3.2 Desempenho de Protocolos DM-CVQKD

Nesta seção, teremos como objetivo realizar uma análise preliminar de como constelações de estados coerentes se comportam em um cenário em que o canal quântico conectando Alice e Bob não apresenta ruído térmico, apenas atenuação do modo de entrada. Mesmo não sendo um caso realista, será um bom ponto de partida para observar quais tipos de constelações aproximam mais rapidamente do limite da modulação gaussiana. A seguir, serão utilizadas as constelações unidimensionais apresentadas na seção anterior.

3.2.1 Protocolo UD-CVQKD com Modulação Discreta[5]

Aqui exploraremos o desempenho das constelações unidimensionais da Seção 3.1.2 aplicadas ao contexto de protocolos CVQKD. Por simplicidade, denotaremos uma constelação arbitrária pela variável aleatória A com alfabeto $\mathcal{A} = \{\alpha_i\}_{i=1}^m$ e distribuição $\mathcal{P} = \{p(\alpha_i)\}_{i=1}^m$, e o protocolo CVQKD com modulação discreta unidimensional (DUD-CVQKD, do inglês: *Discrete Unidimensional CVQKD*) fará uso desta constelação durante toda a etapa de comunicação quântica. Alice e Bob decidem pelo formato de constelação A, bem como sua cardinalidade m. Alice mapeia sequências binárias com $\lceil \log_2(m) \rceil$ bits em estados coerentes pertencentes ao *ensemble* $\mathcal{S} = \{|\alpha_i\rangle, p(\alpha_i)\}_{i=1}^m$. O protocolo funciona da seguinte maneira.

(i) *Preparação dos estados* - Em cada rodada do protocolo, Alice sorteia uma amplitude da constelação e prepara o estado $|\alpha_i\rangle$. A constelação pode ser representada pela

[5]Os resultados desta seção foram publicados na *Quantum Information Processing* [29].

mistura $\hat{\rho}_A = \sum_{\alpha \in \mathcal{A}} p(\alpha) \left|\alpha\right\rangle\!\left\langle\alpha\right|$ e o registrador $\boldsymbol{A'}$ armazena a sequência de valores de amplitudes dos estados transmitidos.

(ii) *Transmissão quântica e medição* - Alice envia os estados preparados por um canal quântico $\mathcal{N}_{A\to B}$ de modo que Bob observe a mistura $\hat{\rho}_B = \mathcal{N}_{A\to B}(\hat{\rho}_A)$ e realize a detecção homódina nos estados recebidos. Os resultados das medições são armazenados no registrador $\boldsymbol{B'}$.

(iii) *Sifting* - Após a conclusão de L rodadas, Alice e Bob concordam em um subconjunto $I_{\text{test}} \subset [L]$ para compor o conjunto de teste a ser utilizado na estimação de parâmetros. Os valores de $\boldsymbol{A'}$ e $\boldsymbol{B'}$ indexados por I_{test} serão anunciados publicamente e então descartados. A chave bruta restante é indexada por $I_{\text{key}} = [L] \setminus I_{\text{test}}$ e representada por $\boldsymbol{A}$ e $\boldsymbol{B}$ para Alice e Bob, respectivamente.

(iv) *Estimação de parâmetros* - Alice e Bob utilizam os conjuntos $\boldsymbol{A}[I_{\text{test}}]$ e $\boldsymbol{B}[I_{\text{test}}]$ para estimar os parâmetros necessários para decidir se as chaves brutas podem gerar chaves seguras, calculando a taxa de chave secreta. Para o presente protocolo, os parâmetros de interesse são a transmitância do canal e o ruído térmico observado no receptor.

(v) *Reconciliação e amplificação de privacidade* - Caso os parâmetros estimados indiquem que é viável destilar uma chave secreta, Alice e Bob devem primeiro corrigir os erros entre suas sequências A e B, as chaves brutas, por meio de um protocolo de reconciliação, normalmente empregando um código corretor de erros. A segunda tarefa será remover uma quantidade de bits proporcional à informação obtida pela espiã, utilizando funções de *hashing*, que é a amplificação de privacidade.

A espiã, por sua vez, está restrita a controlar a transmissividade do canal, conforme esquema da Figura 6. Contudo, seu aparato de medição realiza a detecção coletiva dos estados interceptados, o que implica acesso à memória quântica e dispositivo de detecção de vários modos, permitindo atingir o limitante de Holevo para a informação acessível aos estados recebidos por Bob (reconciliação reversa). A taxa de chave secreta (SKR, do inglês: *Secret Key Rate*) final por estado transmitido para um protocolo com modulação discreta de m estados é dada por

$$K_{(m)} = I(A;B) - \chi(E,B), \tag{3.21}$$

em que $I(A;B)$ é a informação mútua (clássica) de Shannon e $\chi(E,B)$ é o limitante de Holevo que limita a informação quântica de Eva referente aos estados de Bob.

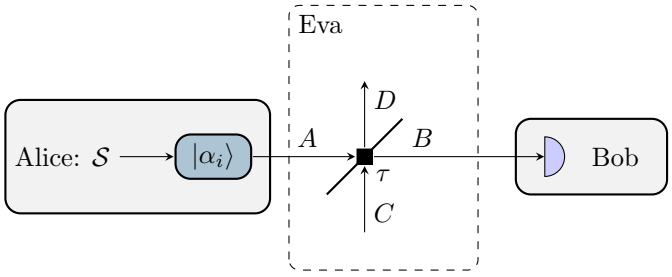


Figura 6 – Modelo do canal quântico sem ruídos.

O cálculo da informação mútua entre Alice e Bob é derivado das variáveis aleatórias ao final da fase quântica. Alice possui uma variável aleatória discreta $A = \{\alpha_i, p_i\}_{i=1}^{m}$ definida pela constelação usada durante a execução do protocolo, e Bob, que realiza detecção homódina, possui uma variável aleatória contínua $B = \{b, p(b)\}$, resultado da medição homódina, relacionada aos estados de Alice da seguinte forma:

$$p(b) = \sum_{i=1}^{m} p(\alpha_i) p(b|\alpha_i), \tag{3.22}$$

sendo $p(b|\alpha_i)$ a distribuição de probabilidade homódina condicionada ao estado $|\alpha_i\rangle$ transmitido pelo canal com transmissividade τ,

$$p(b|\alpha_i) = \frac{e^{-2(b-\sqrt{\tau}\alpha_i)^2}}{\sqrt{\pi/2}}. \tag{3.23}$$

A informação mútua é então dada por

$$\begin{aligned} I(A;B) &= H(A) - H(A|B) \\ &= -\sum_{i=1}^{m} \log(p_i) - \int p(b) H(A|B=b)\, \mathrm{d}b\,, \end{aligned} \tag{3.24}$$

em que $p(\alpha_i|b) = p(\alpha_i)p(b|\alpha_i)/p(b)$.

Na reconciliação reversa, Alice corrige sua chave bruta com relação à sequência de Bob de modo que Eva deve admitir uma mistura de estados condicionada ao resultado b da medição realizada por Bob,

$$\hat{\rho}_{E|b} = \sum_{i=1}^{m} p(\alpha_i|b) \left|\sqrt{1-\tau}\alpha_i\right\rangle\!\left\langle\sqrt{1-\tau}\alpha_i\right|. \tag{3.25}$$

Então, a incerteza média do sistema da espiã condicionado ao sistema de Bob é dada por

$$S(\hat{\rho}_E|B) = \int p(b) S(\hat{\rho}_{E|b})\, \mathrm{d}b\,, \tag{3.26}$$

que resulta em

$$\chi(E,B) = S(\hat{\rho}_E) - S(\hat{\rho}_E|B). \tag{3.27}$$

Taxas de Chave Secreta

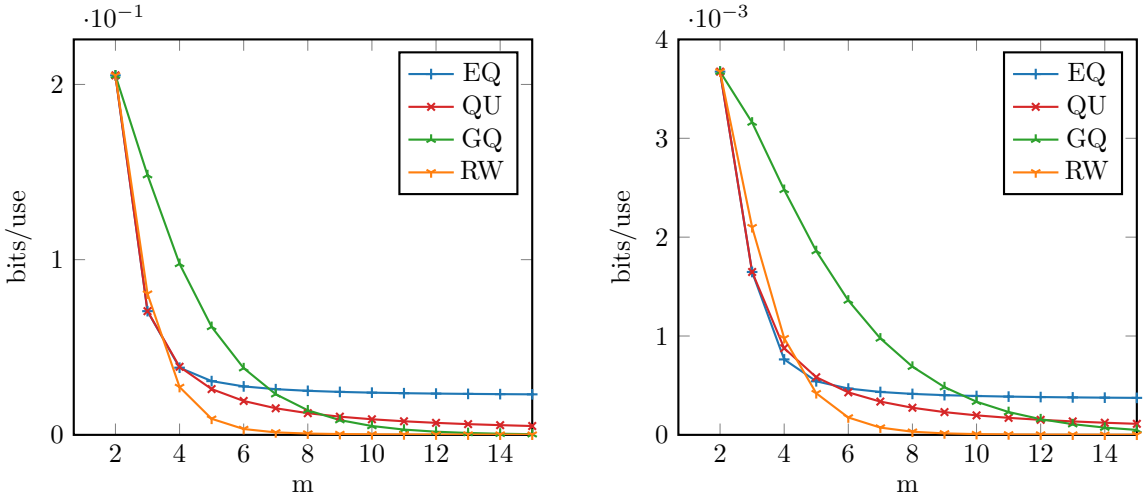
A fim de comparar as performances das quatro constelações apresentadas, inclusive as relacionar com a modulação Gaussiana do protocolo UD-CVQKD (Seção 2.3.2), vamos definir a lacuna de SKR $\Delta K(m) = K_{cont} - K_{(m)}$, a diferença entre a taxa de chave secreta obtida pelo protocolo com modulação Gaussiana e o protocolo com modulação discreta equivalente com m estados quânticos, ambos com a mesma energia média de modulação.

Na Figura 7, estão apresentados os resultados para as lacunas de SKR $\Delta K(m)$ para cada uma das quatro constelações da Seção 3.1.2 considerando $\tau \in \{0.5, 0.01\}$ e variância de modulação unitária tanto para protocolos com modulação discreta como para modulação contínua, $\tilde{V}_m = 1$. Notamos primeiro que ambos os gráficos mostram desempenhos de constelações que se assemelham aos resultados de fechamento da lacuna de capacidade no contexto clássico, obtidos em [26], onde GQ e RW superam EQ e QU. No contexto clássico, para o valor de snrem 0 dB, a constelação GQ converge mais rapidamente para a capacidade do canal AWGN, seguido pelas constelações RW, QU e EQ, nesta ordem, para qualquer m. Em alta snr(10 dB), RW mostra melhor desempenho do que GQ para $m < 25$, uma vez que GQ precisa de mais pontos para realizar a convergência exponencial. Ao lidar com QKD, a snré dada por [59]

$$\mathsf{snr} = \frac{\frac{1}{\mu}\tau\eta V_m}{1 + \frac{1}{\mu}\xi}, \tag{3.28}$$

e, tomando $\xi = 0$ e $\mu = 1$ (indica detecção homódina aplicada), temos que $\mathsf{snr} = 4\tau\eta\tilde{V}_m$. Como os links de longo alcance são de interesse especial, nos concentramos em resultados de snrbaixos. Chamamos a atenção para o fato de que ao lidar com comunicações quânticas, mesmo considerando canais sem ruído, ainda existem flutuações quânticas nos dados medidos devido à própria natureza quântica dos estados coerentes e, como será analisado posteriormente, eficiência quântica na detecção afeta fortemente a relação sinal ruído final. Então, faz sentido em falar sobre snr, mesmo quando se considera canais quânticos sem ruído.

Além de sua semelhança com a lacuna de capacidade clássica, as quatro constelações aplicadas ao QKD têm desempenho muito semelhante tanto para snralto (3 dB) quanto para snrbaixo (-14 dB), com RW apresentando a convergência mais rápida, seguido por GQ. Curiosamente, a lacuna de SKR torna-se ainda menor na medida que a transmitância diminui, sendo da ordem de 10^{-2} bits para $\tau = 0.1$ e 10^{-3} bits para $\tau = 0.01$, implicando que a modulação discreta se aproxima adequadamente de uma modulação Gaussiana em regime de baixa snr. Não mais do que oito estados com uma constelação do tipo RW é suficiente para aproximar a modulação Gaussiana contínua com um erro desprezível.



(a) $\tau = 0.5$ (snr≈ 3 dB) (b) $\tau = 0.01$ (snr≈ -14 dB)

Figura 7 – Lacuna de SKR $\Delta K(m)$ em função de m para diferentes formas de constelação (EQ, QU, GQ e RW). As constelações do tipo GQ e RW atingem o SKR máximo conforme m cresce, sendo a última mais rápida. A constelação de QU parece ter o mesmo comportamento, mas de forma lenta, e EQ satura.

Constelações Ótimas com Quatro Estados

Como apontado por Wu e Verdú em [26], reforçando os resultados conhecidos desde o artigo seminal de Shannon [71], uma constelação de dois estados (sinalização antipodal BPSK) atinge a capacidade de um canal AWGN em regime de baixa snr, sendo suficiente, mas o limite de capacidade (no contexto clássico) é exponencialmente pequeno para qualquer snrquando a cardinalidade da constelação é grande suficiente. Os resultados na Figura 7 mostram que tal comportamento é mantido quando as constelações que alcançam a capacidade clássica do canal são utilizadas nos protocolos DM-CVQKD: as constelações de dois estados resultam em $\Delta K(2) \approx 3.5 \cdot 10^{-3}$ bits com $\tau = 0.01$, enquanto para $\tau = 0.5$, $\Delta K(2) \approx 2 \cdot 10^{-1}$. Entretanto, pode-se ver que a constelação de quatro estados com a menor lacuna de SKR em $\tau = 0.5$ é o RW, que é probabilisticamente formatada e apresenta um desempenho geral ótimo para $4 \leq m \leq 10$ entre as constelações apresentadas, seguido por EQ e QU (que tem formatação geométrica). Isso significa que ainda há espaço para melhorias no desempenho de constelações de pequena cardinalidade aplicando algum tipo de formatação.

Dito isso, focamos em encontrar constelações ideais com quatro estados, realizando uma busca exaustiva sobre as possíveis geometrias na constelação e distribuições de probabilidade. Seja $\mathcal{C}^{(4)}$ o conjunto de todos os conjuntos de quatro estados coerentes de modo que $\mathcal{A} = \{|\alpha_1\rangle, |-\alpha_1\rangle, |\alpha_2\rangle, |-\alpha_2\rangle\}$, $\alpha_i \in \mathbb{R}$ e $\alpha_2 = \lambda\alpha_1$ ($\lambda > 1$), e probabilidade distribuição $\{p, p, q, q\}$, onde $p > q = \frac{1}{2} - p$. Chame $\hat{\rho}_m$ o operador densidade que representa um conjunto arbitrário de $\mathcal{C}^{(4)}$ submetido à restrição de energia

$\mathrm{tr}(\hat{\rho}_m\hat{n}) = \tilde{V}_m$. Defina $I(A;B)(\hat{\rho}_m)$ e $\chi(E,B)(\hat{\rho}_m)$ como sendo a informação mútua de Alice e Bob e a informação acessível de Eva, ambas assumindo que o protocolo usou a constelação representada por $\hat{\rho}_m$. Então, a SKR máxima para um protocolo unidimensional de quatro estados é dado por

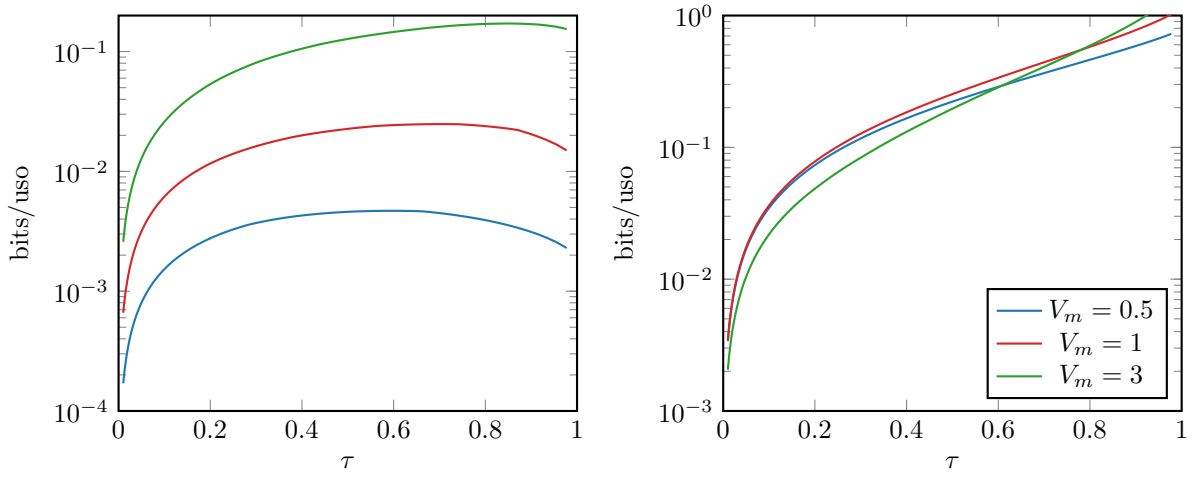
$$K_{max}^{(4)} = \max_{\substack{\hat{\rho}_m \in \mathcal{C}^{(4)} \\ \mathrm{tr}(\hat{\rho}_m\hat{n})=\tilde{V}_m}} \{I(A;B)(\hat{\rho}_m) - \chi(E,B)(\hat{\rho}_m)\}. \tag{3.29}$$

Em seguida, definimos o intervalo SKR mínimo para uma constelação de quatro estados, $\Delta K_{min}^{(4)} = K_{cont} - K_{max}^{(4)}$. A Figura 8 apresenta as curvas de $\Delta K_{min}^{(4)}$ para $\tilde{V}_m \in \{0.5, 1, 3\}$, bem como as taxas ótimas de chave secreta obtidas. Pode-se ver que conforme a lacuna de SKR diminui com $\tilde{V}_m$, quatro estados são suficientes para aproximar uma modulação Gaussiana com $\tilde{V}_m$, especialmente para $\tau < 0.1$ com $\Delta K_{min}^{(4)} < 10^{-3}$ bits. Entretanto, as melhores taxas são atingidas com $\tilde{V}_m = 1$ (Figura 8b). Constelações de quatro estados com $\tilde{V}_m \gg 1$ resultam em baixos valores de SKR, seja quando comparadas com a modulação Gaussiana equivalente (a lacuna de SKR é relativamente grande em quase todas as faixas de transmitância) ou com constelação de energia mais baixa, devido ao fato de que conforme a energia aumenta, torna-se mais fácil distinguir entre os estados. Assim, Bob e Eva podem se beneficiar de constelações de alta energia devido à distinção de estados, mas Eva se sai melhor, pois a taxa de chave é diminuída em quase todos os valores de transmitância.

Outros aspectos interessantes das constelações de quatro estados ótimas são a forma geométrica e probabilista, representada na Figura 9. Como apontado anteriormente, melhores taxas de chave secreta podem ser obtidas alterando as amplitudes dos estados e/ou suas probabilidades *a priori*. Na região curta/média distância ($0.2 \leq \tau < 1$) as melhores constelações resultaram da alteração de α_2 e p, com α_1 fixo. Para longas distâncias ($\tau < 0.2$), a constelação com geometria uniforme e estados não equiprováveis ($p = 0.31$) apresentou a melhor SKR.

Detecção não Ideal

A análise apresentada até agora não levou em consideração nenhum ruído, desde a preparação do estado por parte de Alice até a detecção quântica no laboratório de Bob. Essa suposição limita fortemente a operação de espionagem e não leva em consideração nenhum ruído de modulação ou detecção. Nesta seção, pretendemos explorar como a detecção homódina balanceada (BHD, do inglês: *Balanced Homdyne Detection*) com eficiência quântica não unitária afeta o desempenho do protocolo, tornando a análise dos protocolos DUD-CVQKD mais acurada.



(a) $\Delta K_{min}(4)$ (b) $K^{(4)}_{max}$

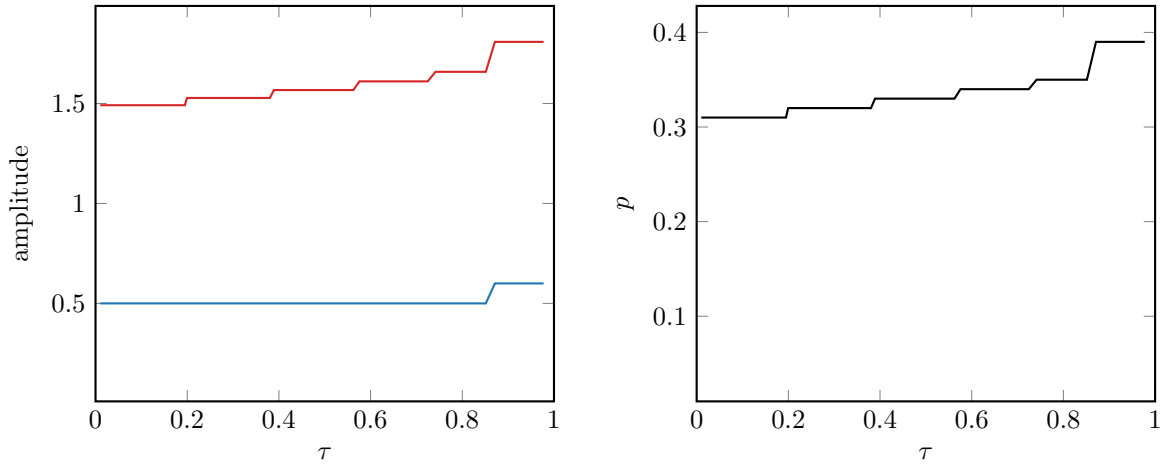
Figura 8 – Valores da lacuna de SKR minimizados (a) e correspondentes valores das taxas de chave secreta maximizada para o protocolo UD-CVQKD com quatro estados calculados de acordo com a Equação (3.29) com $\tilde{V}_m = \{0,5, 1, 3\}$. Apesar de que as constelações com $\tilde{V}_m = 0.5$ resultam nos menores valores da lacuna de SKR, a taxa de chave com $\tilde{V}_m = 1$ alcança maiores taxas de chave. As constelações com $\tilde{V}_m = 3$, apresentam os piores resultados, tanto com relação a $K^{(4)}_{max}$ quanto $\Delta K^{(4)}_{min}$.

Para contabilizar os efeitos da eficiência não unitária de detecção, é necessário ajustar o cálculo da taxa de chave secreta para os protocolos considerados. De um modo geral, detectores com eficiência não unitária aumentam a variância da distribuição normal que representa a detecção de estados coerentes, conforme desenvolvido na Apêndice A.3.4. A saída de um BHD com eficiência quântica η na detecção de um estado coerente α que foi transmitido por um canal quântico sem ruído com transmissividade τ é uma variável aleatória contínua com distribuição normal $X \sim \mathcal{N}(\sqrt{\tau}\alpha, 1/4\eta)$.

Para inserir o efeito do BHD não unitário ao protocolo UD-CVQKD, basta tomar o modelo do protocolo EB equivalente e considerar que o canal é realizado por um *beam splitter* com transmissividade $\tau\eta$, sendo η a eficiência do BHD.

Dessa maneira, a matriz de covariância $\mathbf{\Sigma}'$ do estado compartilhado por Alice e Bob será

$$\mathbf{\Sigma}''_{AB} = \begin{pmatrix} V & 0 & \sqrt{\tau\eta}\sqrt{V(V^2-1)} & 0 \\ 0 & V & 0 & -\sqrt{\tau\eta}\sqrt{\frac{V^2-1}{V}} \\ \sqrt{\tau\eta}\sqrt{V(V^2-1)} & 0 & 1+\tau\eta(V_m+\xi) & 0 \\ 0 & -\sqrt{\tau\eta}\sqrt{\frac{V^2-1}{V}} & 0 & 1+\tau\eta\xi \end{pmatrix}, \quad (3.30)$$



(a) Valores ótimos das amplitudes α_1 e α_2.

(b) Valores ótimos de p.

Figura 9 – Parâmetros α_1, α_2 e p para os *ensembles* que maximizam a taxa de chave secreta na Equação (3.29) considerando $\tilde{V}_m$. A otimização combina formatação geométrica e probabilística e resulta em diferentes constelações para cada transmissividade. Na região com $\tau > 0.2$, os melhores valores de SKR são obtidos com ajustes em α_2 e p enquanto para $\tau < 0.2$, constelações com estados igualmente espaçados não equiprováveis ($p > q$) leva aos melhores resultados.

$$= \begin{pmatrix} \boldsymbol{A} & \boldsymbol{C'} \\ \boldsymbol{C'}^T & \boldsymbol{B'} \end{pmatrix}. \tag{3.31}$$

A Figura 10 mostra as curvas de SKR para o protocolo UD-CVQKD e para o

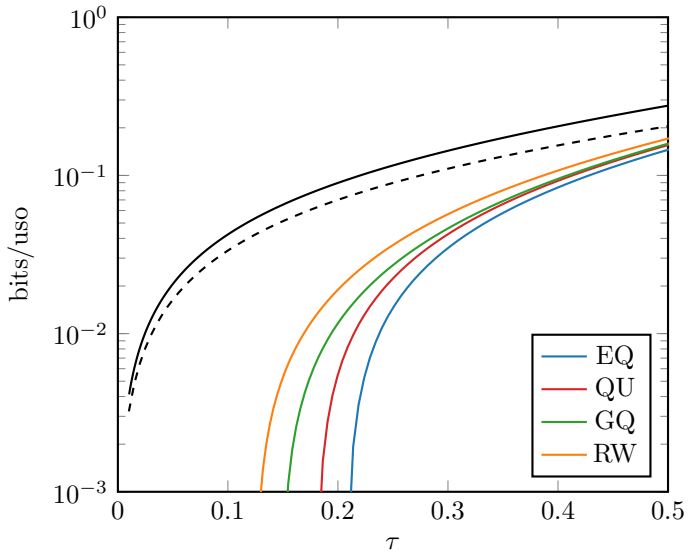
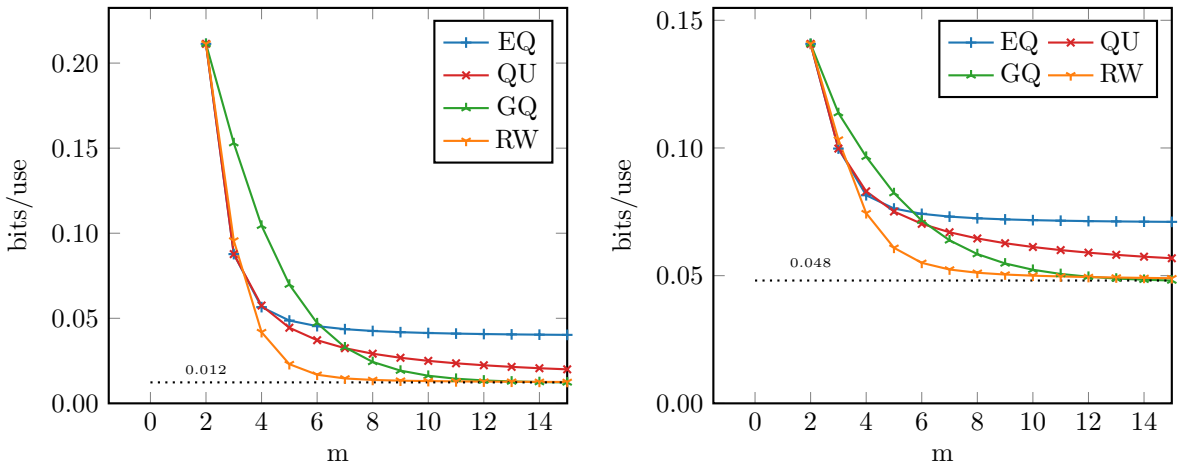


Figura 10 – Taxas de chave secreta para os protocolo UD-CVQKD e DUD-CVQKD com as constelações da Seção 3.1.2 com $\eta = 0.8$ e $\tilde{V}_m = 1$. As curvas sólidas e tracejadas superiores correspondem à modulação gaussiana ($\eta = 1$ e $\eta = 0.8$, respectivamente) enquanto as demais correspondem às modulações discretas com oito estados e $\eta = 0.8$.



(a) $\tau = 0.6$ (snr$\approx$ 2.8 dB) (b) $\tau = 0.2$ (snr≈ -1.93 dB)

Figura 11 – Lacuna de SKR $\Delta K(m)$ para os quatro tipos de constelações (GQ, RW, QU e EQ), considerando a eficiência quântica de detecção $\eta = 0.8$.

protocolo DUD-CVQKD com oito estados utilizando as constelações da Seção 3.1.2, considerando $\eta = 0.8$ e $\tilde{V}_m = 1$. Os resultados mostram que os efeitos da eficiência quântica não unitária do BHD se tornam mais severos para a modulação discreta conforme a transmitância do canal diminui, de modo que a execução do protocolo se torna inviável para $\tau < 0.1$. Pode-se observar que a constelação RW tem melhor desempenho, mantendo as melhores taxas de chave secreta e atingindo o maior alcance, seguida pelas constelações GQ, QU e EQ, nessa sequência.

Na Figura 11, plotamos as curvas de SKR $\Delta K(m)$ para as transmitâncias $\tau = \{0.6, 0.2\}$, ainda assumindo $\eta = 0.8$. Os resultados mostram que os padrões observados para $\eta = 1$ da Figura 7 são mantidos, ou seja, as constelações com melhor desempenho no cenário perfeito performam melhor quando $\eta < 1$. No entanto, a detecção não ideal parece impor uma lacuna de SKR fundamental que não pode ser superada com o aumento da cardinalidade da constelação, além de que essa lacuna aumenta com a distância: a lacuna de SKR para $\tau = 0.2$ é quatro vezes o valor da lacuna para $\tau = 0.6$. Ambas as constelações GQ e RW minimizam a lacuna de SKR com o aumento de m, mas atingir seu valor mínimo exige constelações maiores. Ressaltamos que RW ainda converge mais rápido que todos os outros tipos de constelação, onde oito estados parecem ser suficientes em quase todos os cenários.

Também notamos que os valores snrdados pela Equação (3.28) não representam um parâmetro absoluto para comparar a habilidade das constelações de "fechar a lacuna". Na verdade, a eficiência de detecção acaba sendo muito mais significativa no desempenho da modulação discreta, uma vez que N grande é suficiente para fechar a lacuna quando admitimos $\eta = 1$, embora não seja verdade para os casos em que $\eta < 1$, conforme

discutido anteriormente. As constelações GQ e RW mostraram ser capazes de fechar a lacuna para qualquer transmitância se $\eta = 1$. Enquanto isso, pode-se observar que existe uma correlação entre o nível snre a lacuna mínima do SKR, quando $\eta < 1$. A Figura 11 mostra que uma diminuição de 4.73 dB no snrresultou em um aumento de 4 vezes na lacuna de SKR.

3.2.2 Constelações APSK[6]

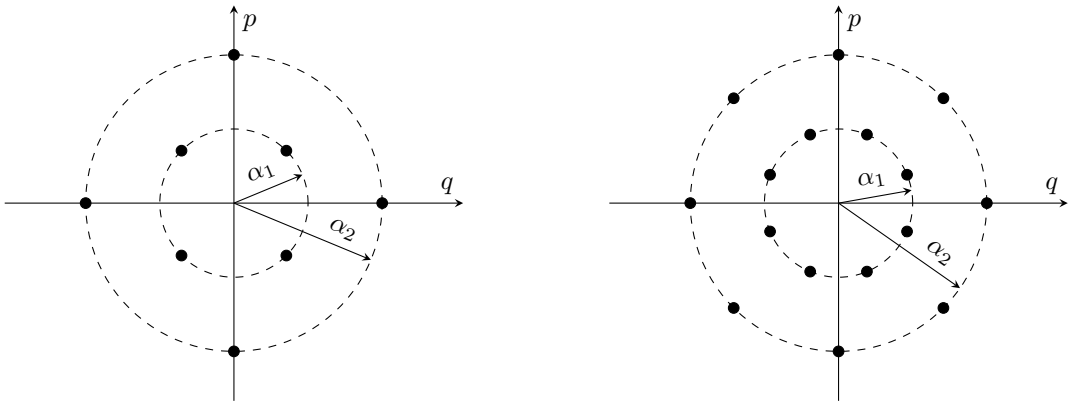
Nas seções anteriores, abordamos alguns modelos de constelações unidimensionais que alcançam a capacidade do canal AWGN (comunicações clássicas). Contudo, de acordo com a Equação (3.3), é possível transmitir mais informação utilizando esquemas de modulação bidimensional (PSK, QAM, etc.), e a aproximação da capacidade do canal (fechamento da lacuna) é possível utilizando constelações com formatação geométrica e probabilística, conforme visto na seção anterior, em que constelações que aplicam algum tipo de formatação superam o desempenho de constelações uniformes. Nesta seção, apresentaremos uma constelação com modulação em amplitude e fase baseada nos resultados da Seção 3.2.1 e compararemos seu desempenho para protocolos DM-CVQKD com constelações PSK, APK e QAM com até 16 estados.

As constelações ótimas de quatro estados da Seção 3.2.1 foram obtidas pela busca exaustiva em cada valor de transmitância pelos parâmetros α_1, α_2 e p que maximizam a taxa de chave secreta. Os valores de cada parâmetro encontrado estão na Figura 9. Percebe-se que, na faixa de transmitância $\tau < 0.5$, α_1 não sofre alterações, e α_2 e p são ligeiramente ajustados de modo que as melhores taxas de chave secreta para enlaces de longa distância (sob a hipótese de um canal sem ruídos) são alcançadas por meio de constelações com formatação geométrica e probabilística.

Para construir constelações bidimensionais ótimas, usamos os parâmetros para projetar esquemas de modulações em fase e amplitude ótimos (OAPSK, do inglês: *Optimal* APSK) com oito e dezesseis estados. Denotamos por N_1/N_2 OAPSK a constelação de amplitude-fase deslocada com N_1 estados de energia α_1^2 e N_2 estados de energia α_2^2. A partir das probabilidades $\{p_1, p_2\}$, definimos que o estado com energia α_i^2 é preparado com probabilidade $q_i = 2p_i/N_i$. Essas constelações são mostradas em Figura 12.

Ajustando as Equações (3.24) e (3.25) com a probabilidade de detecção heteródina

[6]Os resultados desta seção foram publicados nos anais do XXXIX SIMPÓSIO BRASILEIRO DE TELECOMUNICAÇÕES E PROCESSAMENTO DE SINAIS - SBrT 2021. *Pre-print* disponível em [72].



(a) (b)

Figura 12 – Constelações OAPSK com oito (a) e dezesseis (b) estados projetadas a partir das constelações unidimensionais ótimas da Equação (3.29).

de Bob condicionada ao estado α_i enviado por um canal com transmitância τ,

$$p(b|\alpha_i) = \frac{1}{\pi} e^{-|b-\sqrt{\tau}\alpha_i|^2}, \tag{3.32}$$

as taxas de chave secreta são calculadas analogamente aos protocolos unidimensionais.

Na Figura 13, plotamos o SKR para as constelações OAPSK de oito e dezesseis estados junto com as constelações 8PSK, 16PSK, 4/4APSK, 8/8APSK e 16QAM convencionais (símbolos uniformemente espaçados e equiprováveis). A princípio, os resultados mostram que as constelações propostas, aplicadas a protocolos DM-CVQKD, superam os protocolos baseados em constelações PSK e APK. Comparando as constelações com oito estados, o protocolo com constelação 4/4OAPSK resulta em taxas de chave mais altas em toda a faixa de transmitância e também atinge distâncias maiores (SKRs positivos para baixas transmitâncias). Quando nos voltamos para o protocolo proposto de dezesseis estados, duas coisas chamam a atenção. Primeiro, aumentar a cardinalidade da constelação proposta aumenta consideravelmente a taxa de chave secreta, e segundo, não há diferença significativa entre as constelações 8PSK e 16PSK. A constelação 16APSK apresenta um aprimoramento de desempenho, mas tem desempenho inferior às constelações 4/4OAPSK e 8/8OAPSK. Pode-se concluir que os protocolos baseados em m-PSK possuem um ponto de saturação em sua cardinalidade próximo a oito estados. Comparando a constelação APK tradicional e nossas constelações OAPSK propostas, podemos concluir que ajustes simples na geometria da constelação e na distribuição de probabilidade resultam em um aumento considerável do SKR e permite que o protocolo alcance distâncias maiores.

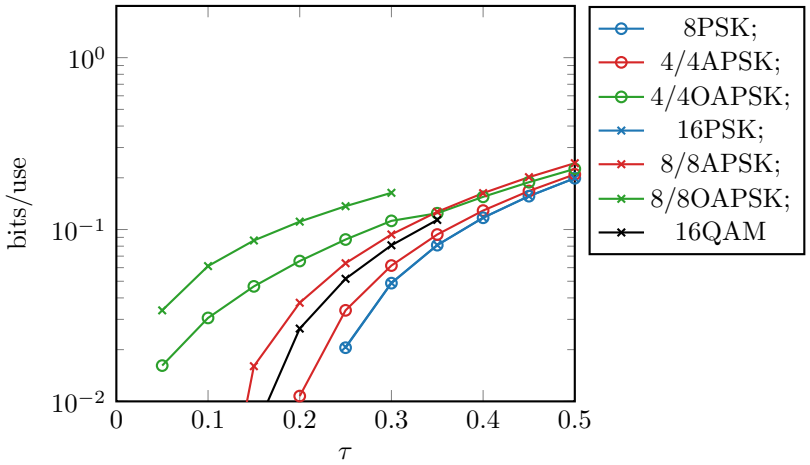


Figura 13 – Taxas de chave secreta para protocolos DM-CVQKD baseados em constelações PSK, APK, QAM e nas OAPSK propostas. As constelações de oito e dezesseis estados são diferenciadas pelos marcadores (círculos e constelações, respectivamente) e todas foram fixadas para energia média unitária.

3.3 Limitante Inferior para Canais Arbitrários

A análise realizada na Seção 3.2 levou em consideração um canal quântico linear sem ruído, o que é equivalente a considerar um canal gaussiano com ruído térmico nulo [48]. O objetivo era observar, no caso mais simples possível, se as constelações apresentadas na Seção 3.1.2 poderiam ser utilizadas para definir um protocolo DM-CVQKD que aproxima o desempenho de uma modulação contínua gaussiana. A resposta obtida é positiva – a diferença de taxa de chave secreta entre a modulação discreta e contínua gaussiana (ambas unidimensionais) cai exponencialmente com o aumento da cardinalidade das constelações. Em especial, as constelações baseadas na quadratura de Gauss e em passeios aleatórios normalizados apresentam os melhores resultados.

Nesta seção, iremos utilizar os resultados desenvolvidos em [30] para expandir a análise das constelações considerando canais arbitrários, mantendo a hipótese de ataques coletivos. A Seção 3.3.1 apresenta a purificação da constelação e um limitante inferior para a taxa de chave secreta considerando canais arbitrários. Os resultados finais deste capítulo são apresentados na Seção 3.3.2 onde o desempenho de constelações resultantes do produto cartesiano das constelações unidimensionais já analisadas são comparados.

3.3.1 Protocolo EB Equivalente

Para calcular as taxas de chave secreta de protocolos DM-CVQKD sem impor restrições ao canal quântico conectando Alice e Bob, é necessário estabelecer o protocolo

baseado em emaranhamento[7] equivalente ao esquema "prepara e mede" definido na Seção 3.2.1. O primeiro passo consiste na purificação da constelação. Considere uma constelação definida pela variável aleatória X com alfabeto complexo $\mathcal{X}$, $|\mathcal{X}| = m^2 = N$, cujos elementos são representados por $x = \alpha_1 + j\alpha_2$, $\alpha_1, \alpha_2 \in \mathcal{A}$, sendo $\mathcal{A}$ uma das constelações unidimensionais definidas na Seção 3.1.2. O operador densidade $\hat{\rho}_A = \sum_{x\in\mathcal{X}} p(x) |x\rangle\langle x|$ representa a constelação de estados coerentes preparados por Alice, a qual, sem perda de generalidade, também pode ser representada pela decomposição espectral.

$$\hat{\rho}_A = \sum_{k=1}^{N} \lambda_k |\phi_k\rangle\langle\phi_k| , \tag{3.33}$$

Agora, defina a seguinte purificação:

$$|\Phi\rangle_{AA'} = (\mathbb{1} \otimes \hat{\tau}^{1/2}) \sum_{n=0}^{\infty} |n\rangle |n\rangle \tag{3.34}$$

$$\stackrel{a}{=} \left[\mathbb{1} \otimes \left(\sum_{k=1}^{N} \lambda_k^{1/2} |\phi_k\rangle\langle\phi_k|\right)\right] \sum_{n=0}^{\infty} |n\rangle |n\rangle \tag{3.35}$$

$$\stackrel{b}{=} \sum_{n=0}^{\infty} |n\rangle \otimes \left(\sum_{k=1}^{N} \lambda_k^{1/2} |\phi_k\rangle \langle\phi_k|n\rangle\right) \tag{3.36}$$

$$\stackrel{c}{=} \sum_{n=0}^{\infty} \sum_{k=1}^{N} \lambda_k^{1/2} \langle\phi_k|n\rangle |n\rangle \otimes |\phi_k\rangle \tag{3.37}$$

$$\stackrel{d}{=} \sum_{k=1}^{N} \lambda_k^{1/2} \left|\bar{\phi}_k\right\rangle |\phi_k\rangle \tag{3.38}$$

em que em (a) usamos a decomposição espectral de $\hat{\rho}_A$, em (b) a propriedade associativa do produto tensorial, e em (d) a conjugação na base de Fock: $|\phi_k\rangle = (\phi_{k,0}, \phi_{k,1}, \phi_{k,2}, \cdots)^T$, $\langle\phi_k|n\rangle = \bar{\phi}_{k,n}$ e então, $\left|\bar{\phi}_k\right\rangle = (\bar{\phi}_{k,0}, \bar{\phi}_{k,1}, \bar{\phi}_{k,2}, \cdots)^T$. É possível então definir o projetor $\Pi = \sum_{k=1}^{N} \left|\bar{\phi}_k\right\rangle\!\left\langle\bar{\phi}_k\right|$ e obter $(\bar{\tau}^{-1/2} \otimes \mathbb{1}) |\Phi\rangle = (\Pi \otimes \mathbb{1}) \sum_{n=0}^{\infty} |n\rangle |n\rangle = \sum_{k=1}^{N} \left|\bar{\phi}_k\right\rangle |\phi_k\rangle$. Definindo o estado $|\psi_k\rangle = \sqrt{p_k}\hat{\rho}_A^{-\frac{1}{2}} |\alpha_k\rangle$, temos que

$$\sum_{k=1}^{N} |\psi_k\rangle\langle\psi_k| = \Pi = \sum_{k=1}^{N} \left|\bar{\phi}_k\right\rangle\!\left\langle\bar{\phi}_k\right| , \tag{3.39}$$

e então o conjunto $\{|\psi_k\rangle\}$ forma uma base ortonormal para o subespaço gerado por pelos estados coerentes da constelação. Isso permite reescreer a purificação da Equação (3.34)

[7] O cenário em que o canal não apresenta ruído térmico possibilita calcular as entropias de von Neumann das constelações sem a necessidade de truncar o espaço de Hilbert, uma vez que a entropia das misturas de estados puros na entrada e saída do canal pode ser calculada pelas respectivas matrizes de Gram normalizadas. O mesmo procedimento não pode ser aplicado quando se considera um canal com ruído térmico, que mapeia estados coerentes em estados térmicos deslocados. Portanto, para o caso geral, aplicamos o procedimento comum nas análises de segurança de protocolos QKD ao definir um estado emaranhado equivalente.

como

$$|\Phi\rangle_{AA'} = \sum_{k=1}^{N} \sqrt{p_k}\, |\psi_k\rangle\, |\alpha_k\rangle\,. \tag{3.40}$$

A forma da purificação de $\hat{\rho}_A$ obtida na Equação (3.40) é importante operacionalmente, pois mostra que a base ortonormal $\{|\psi_k\rangle\}$ deve ser utilizada para construir um conjunto de POVMs (do inglês, *Positive Operator Valued Measurement*) com elementos $M_k = |\psi_k\rangle\langle\psi_k|$ aplicados ao primeiro modo do estado $|\Phi\rangle\langle\Phi|_{AA'}$ e que projetam o segundo modo em um estado coerente da constelação. O canal quântico conectando Alice e Bob, por sua vez, é representado pelo mapa $\mathcal{N}_{A'\to B}$, de modo que o estado compartilhado será

$$\hat{\rho}_{AB} = (\mathbb{1}_A \otimes \mathcal{N}_{A'\to B})(|\Phi\rangle\langle\Phi|_{AA'}), \tag{3.41}$$

e a taxa de chave secreta é dada por

$$K = I(X;Y) - \sup_{\mathcal{N}_{A'\to B}} \chi(Y;E). \tag{3.42}$$

em que o supremum indica uma busca no conjunto de todos os canais quânticos compatíveis com os parâmetros estimados no protocolo "prepara e mede". O sistema de Eva pode ser inserido no modelo considerando uma representação isométrica do canal principal, $\mathcal{U}_{A'\to BE}$, de modo que o sistema tripartido é representado pelo estado

$$\hat{\rho}_{ABE} = (\mathbb{1}_A \otimes \mathcal{U}_{A'\to BE})(|\Phi\rangle\langle\Phi|_{AA'}). \tag{3.43}$$

Calcular o termo $\sup_{\mathcal{N}A'\to B} \chi(Y;E)$ é inviável, uma vez que o espaço de Hilbert que descreve os sistemas tem dimensão infinita. Uma solução é obter um limitante superior utilizando a propriedade da extremalidade dos estados gaussianos (Teorema B.21) (GET, do inglês: *Gaussian Extremality Theorem*), a qual garante que $\chi(Y;E)(\hat{\rho}^G_{ABE}) \geq \chi(Y;E)(\hat{\rho}_{ABE})$, em que $\hat{\rho}^G_{ABE}$ é o estado gaussiano equivalente a $\hat{\rho}_{ABE}$ (Definição B.20). Dessa maneira, é possível calcular $\chi(Y;E)(\hat{\rho}^G_{ABE})$, uma vez que depende apenas da matriz de covariância $\mathbf{\Gamma}$ e, como $\hat{\rho}_{ABE}$ é uma purificação de $\hat{\rho}_{AB}$, $S(\hat{\rho}_{ABE}) = S(\hat{\rho}_{AB})$.

Utilizando argumentos de simetria[8] [34, Apêndice D], é possível garantir que a matriz de covariância $\mathbf{\Gamma}$ tem a seguinte forma,

$$\mathbf{\Gamma} \equiv \begin{bmatrix} V\boldsymbol{I} & Z\boldsymbol{\sigma}_z \\ Z\boldsymbol{\sigma}_z & W\boldsymbol{I} \end{bmatrix}, \tag{3.44}$$

[8]Por "argumentos de simetria", nos referimos à análise da forma geral da matriz de covariância do estado bipartido, em que o termo de covariância se torna independente do ângulo de rotação no espaço de fase, e não tem relação com os processos de simetrização que podem ser considerados na redução de ataques arbitrários para ataques coletivos e serão discutidos no Capítulo 6.

em que

$$V = \frac{1}{2}(\langle \hat{x}_A^2 \rangle + \langle \hat{p}_A^2 \rangle) = 1 + 2\,\mathrm{tr}(\hat{\rho}_{AB}\hat{a}^\dagger\hat{a}), \tag{3.45}$$

$$W = \frac{1}{2}(\langle \hat{x}_B^2 \rangle + \langle \hat{p}_B^2 \rangle) = 1 + 2\,\mathrm{tr}(\hat{\rho}_{AB}\hat{b}^\dagger\hat{b}), \tag{3.46}$$

$$Z = \frac{1}{4}(\langle\{\hat{x}_A, \hat{x}_B\}\rangle - \langle\{\hat{p}_A, \hat{p}_B\}\rangle) = \mathrm{tr}(\hat{\rho}_{AB}(\hat{a}\hat{b} + \hat{a}^\dagger\hat{b}^\dagger)). \tag{3.47}$$

A única quantidade não trivial a ser estimada é $Z = \mathrm{tr}(\hat{\rho}_{AB}\hat{C})$, pois V é um parâmetro do protocolo e W pode ser medido por Bob. Primeiramente, devemos destacar que $\hat{\rho}_{AB}$ não é utilizado na prática, sendo mais uma "conveniência matemática". O protocolo realmente realizado é o de P&M, e o EB é uma equivalência em um cenário hipotético em que Alice tem acesso a $|\Phi\rangle_{AA'}$, e serve apenas para fornecer uma estrutura na qual a segurança do protocolo pode ser avaliada. Portanto, Alice e Bob utilizam o protocolo P&M para compartilhar a chave e precisam reconstruir a matriz de covariância do estado bipartido equivalente *como se tivessem* realizado o protocolo EB.

Em [30], são derivados limitantes inferiores e superiores para Z utilizando o método da soma de quadrados, de modo que

$$Z \geq Z^* = 2c_1 - 2\left(\left(\bar{n}_B - \frac{c_2^2}{\bar{m}}\right)w\right)^{\frac{1}{2}} \tag{3.48}$$

sendo

$$c_1 = \mathrm{Re}\left\{\sum_{i=1}^{N} p(\alpha_i)\,\overline{\langle\alpha_i|\hat{a}_{\rho_A}|\alpha_i\rangle}\beta_i\right\}, \qquad c_2 = \mathrm{Re}\left\{\sum_{i=1}^{N} p_i\bar{\alpha}_i\beta_i\right\}, \tag{3.49}$$

$$w = \sum_{i=1}^{N} p_i\big(\,\langle\alpha_i|\hat{a}_{\rho_A}^\dagger\hat{a}_{\rho_A}|\alpha_i\rangle - |\,\langle\alpha_i|\hat{a}_{\rho_A}|\alpha_i\rangle\,|^2\big), \qquad \hat{a}_{\rho_A} = \hat{\rho}_A^{\frac{1}{2}}\hat{a}\hat{\rho}_A^{-\frac{1}{2}}. \tag{3.50}$$

As quantidades c_1, c_2 e w podem ser estimadas durante a execução do protocolo, utilizando um conjunto de teste grande o suficiente. Vale destacar que, até a data de redação deste trabalho, não foram desenvolvidos estudos relativos à velocidade de convergência dos parâmetros estimados. A expressão da Equação (3.48) não impõe restrições ao canal quântico que conecta Alice e Bob, de modo que a taxa de chave secreta calculada é referente a um canal arbitrário. Para o caso especial de fibras ópticas, que depende apenas da transmissividade e ruído térmico, é obtida a seguinte expressão para o termo de covariância,

$$Z^*(\tau, \xi) = 2\sqrt{\tau}\,\mathrm{tr}(\hat{\rho}_A^{\frac{1}{2}}\hat{a}\hat{\rho}_A^{-\frac{1}{2}}\hat{a}^\dagger) - \sqrt{2\tau\xi w}, \tag{3.51}$$

o qual retorna a expressão padrão da equação Equação (2.12) quando utilizado um esquema de modulação gaussiana. Na próxima seção serão apresentados os resultados das taxas de chave secreta para constelações do tipo m-QAM com formatação obtidas pelo produto cartesiano das constelações unidimensionais apresentadas na Seção 3.1.2.

Tabela 2 – Valores otimizados de ν utilizados nos resultados da Figura 16.

m^2	16	64	256	1024
ν	0.0859	0.0723	0.0315	0.00783

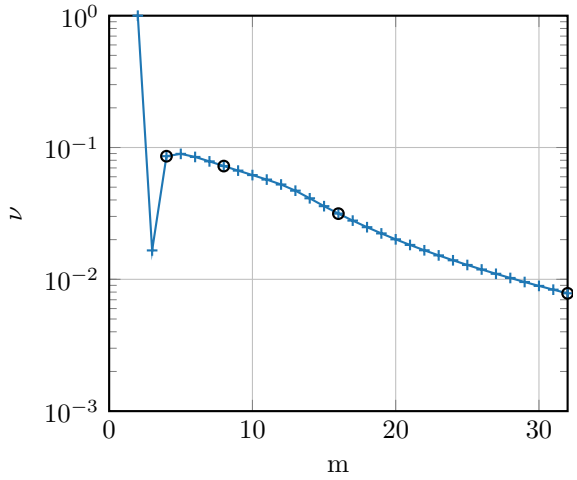


Figura 14 – Valores otimizados de ν para cada valor de m utilizados na Figura 15.

3.3.2 Resultados numéricos

Os resultados numéricos utilizando $Z^*(\tau, \xi)$ estão apresentados nas Figuras 15 e 16. A primeira mostra a lacuna de SKR calculada para $D = 50$ km e dois valores de ruído de excesso (0.02 e 0.1, respectivamente) como função da cardinalidade das constelações ($N = m^2$), e a segunda figura mostra a taxa de chave secreta em função da distância, com ruído de excesso e energia média de modulação fixados em $\xi = 0.02$ e $\bar{m} = 2.5$ (exceto para as constelações 16QAM, em que $\bar{m} = 1$). Foram utilizadas as constelações unidimensionais GQ e RW, analisadas na Seção 3.2, e também a constelação formada pela distribuição gaussiana discreta (DG), utilizada em [30], cujos pontos são dados pela expressão

$$p_{q,p} \sim \exp\{-\nu(q^2 + p^2)\} \tag{3.52}$$

em que o parâmetro ν deve ser otimizado para maximizar a taxa de chave secreta, e o espaçamento entre os pontos é fixado pela energia de modulação. Os valores do parâmetro ν otimizado utilizado nos resultados estão apresentados na Tabela 2 e na Figura 14.

Com relação à lacuna de SKR, podemos verificar que os resultados apresentados na Figura 7 mantêm o mesmo padrão para constelações do tipo QAM, considerando ruído no canal. Comparando os três formatos de constelações (RW, DG e GQ), observamos que a diferença entre modulação discreta e contínua gaussiana diminui mais rapidamente para DG e RW, sendo que DG sempre tem um desempenho melhor no intervalo de cardinalidade analisado. Contudo, os gráficos mostram que a constelação DG não apresenta ganhos

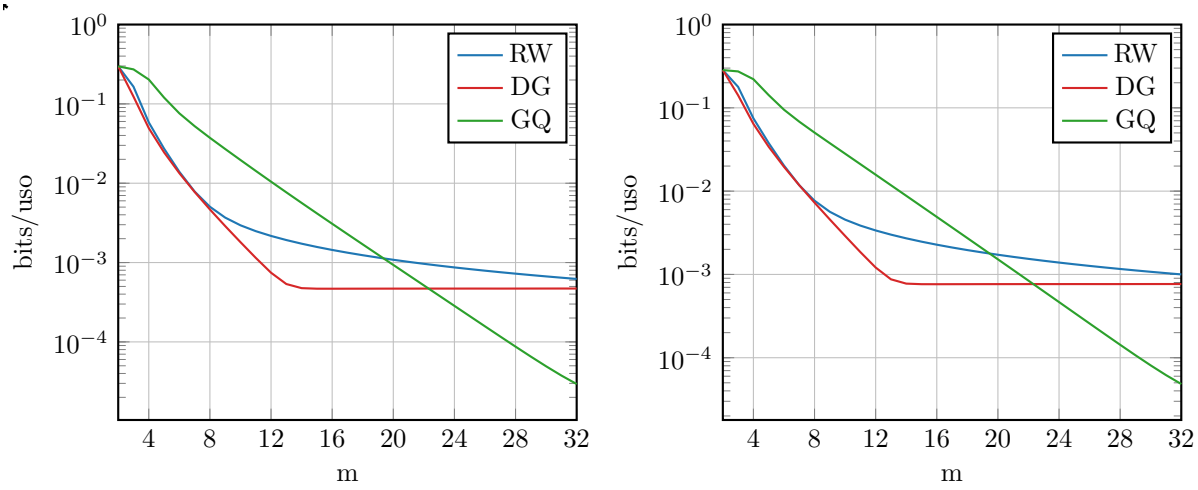


Figura 15 – Lacuna de SKR $\Delta K(m^2)$ calculada para as constelações GQ, RW, DG em função da cardinalidade das constelações $N = m^2$. Foram considerados canais gaussianos com distância $D = 50$km e ruído de excesso (a) $\xi = 0.1$ e (b) $\xi = 0.02$. O parâmetro ν da constelação DG foi otimizado para cada valor de m.

significativos para $m \geq 15$ e há um aparente comportamento decrescente da constelação RW. A constelação do tipo GQ apresenta valores menores de $\Delta K(m^2)$ do que as demais para $m \geq 23$. O aumento do ruído de excesso não resulta em mudanças significativas na comparação entre as constelações, apenas diminui o desempenho geral dos protocolos.

Na Figura 16, constam as taxas de chave secreta como função da distância entre Alice e Bob (em quilômetros) para as constelações RW, DG e GQ, com tamanhos de constelações iguais a 16, 64, 256 e 1024 pontos. Em todos os cenários, foi considerado $\bar{m} = 2.5$ e $\xi = 0.02$ (com exceção das constelações 16QAM, em que $V = 1$), e o parâmetro ν da constelação DG foi otimizado para cada cardinalidade, maximizando a taxa de chave secreta. É possível observar que as constelações DG e RW apresentam resultados semelhantes, como já indicado em [30]. Com relação à constelação GQ, já era esperado, a partir da Figura 15, que os resultados seriam superiores às demais constelações para $m \geq 23$ (529 pontos). Contudo, é possível verificar na Figura 16d que a taxa de chave secreta da constelação GQ é praticamente indistinguível da modulação contínua gaussiana, sendo inclusive superior às taxas para as constelações RW e DG.

Protocolos CVQKD com Modulação Discreta

Neste capítulo, abordamos como esquemas de modulação não gaussiana baseados em constelações de estados coerentes podem ser utilizados no contexto de protocolos

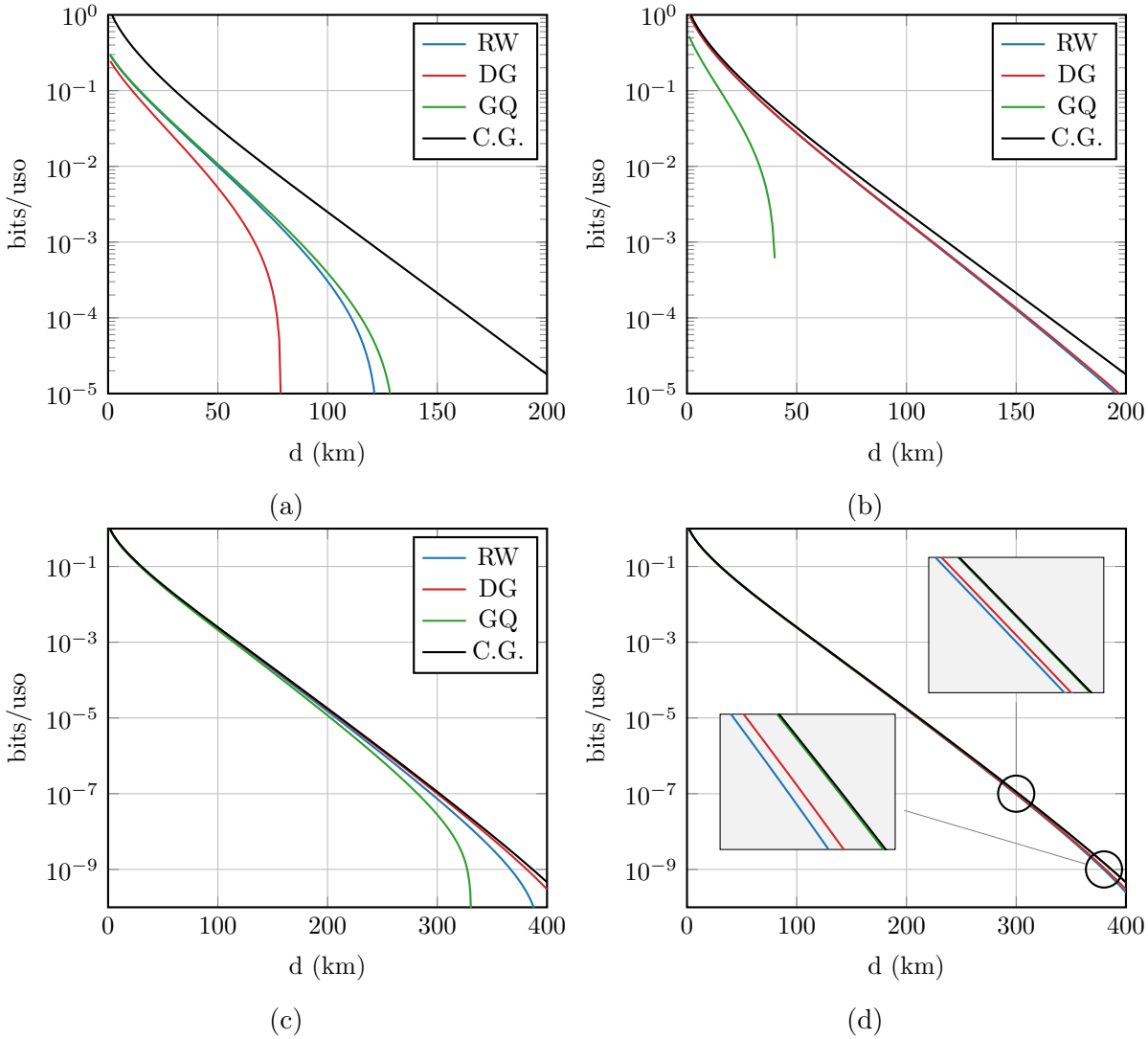


Figura 16 – Taxas de chave secreta calculadas para as constelações RW, GQ e DG com parâmetros (a) $\bar{m} = 1$ e $m = 4$, (b) $\bar{m} = 5$ e $m = 8$, (c) $\bar{m} = 2.5$ e $m = 16$, (d) $\bar{m} = 2.55$ e $m = 32$. Em todos os casos, foi utilziado $\xi = 0.02$. A curva superior em preto representa a taxa de chave secreta acalculada para a modulação gaussiana contínua.

CVQKD, resultando nos protocolos DM-CVQKD. Foram apresentados quatro tipos de constelações unidimensionais com a propriedade de alcançar a capacidade do canal gaussiano nas comunicações clássicas, considerando o limite assintótico do aumento da cardinalidade. Foi mostrado que o uso dessas constelações nos protocolos DM-CVQKD aproxima o desempenho da modulação gaussiana unidimensional em um canal sem ruídos. Ainda sob a hipótese de canais sem ruídos, foi analisado o efeito da detecção com eficiência quântica não unitária nos protocolos DM-CVQKD com constelações unidimensionais, e o desempenho de constelações quaternárias unidimensionais ótimas, bem como constelações APSK com oito e dezesseis estados. As constelações QAM com

formatação geométrica e probabilística foram exploradas para canais ruidosos, e foi observado que, analogamente ao caso unidimensional, o aumento da cardinalidade das constelações aproxima o efeito da modulação gaussiana. Em especial, as constelações com formatação probabilística (gaussiana discreta) e formatação híbrida geométrica-probabilística (Gauss-Hermite) resultam nas melhores aproximações da modulação gaussiana contínua. No próximo capítulo, abordaremos o tema da compatibilidade dos esquemas de formatação probabilística de constelações com a segurança de protocolos QKD, assim como a proposta de um protocolo de reconciliação que realiza a extração de sequências de *bits* independentes e equiprováveis de fontes não equiprováveis.

Capítulo 4

Formatação e Segurança

Neste capítulo, abordaremos o uso de constelações formatadas de um ponto de vista prático, discutindo como a arquitetura usual de um sistema de comunicações ópticas se aplica aos protocolos QKD e quais os possíveis problemas de segurança que podem surgir. Na seção 4.1, discutiremos as principais características de um sistema de comunicações com constelações formatadas, especialmente a formatação probabilística, e como essas técnicas podem comprometer a segurança do protocolo contra ataques arbitrários. Em seguida, na seção 4.2, apresentaremos uma proposta de método de reconciliação de informações que pode evitar os problemas inerentes à arquitetura PAS/PCS.

4.1 Questões Práticas da Formatação de Constelação

Os resultados apresentados no Capítulo 3 mostraram que o uso de constelações com formatação geométrica e/ou probabilística supera a sinalização uniforme equiprovável de constelações do tipo QAM. Além disso, as curvas das Figuras 7 e 15 (unidimensional e QAM, respectivamente) mostraram que a lacuna de capacidade (D_m) do canal AWGN e a lacuna de SKR (ΔK) do protocolo DM-CVQKD têm comportamentos análogos, ou seja, apresentam uma queda exponencial com o aumento da cardinalidade das constelações, e as constelações que têm um bom desempenho no cenário clássico tendem a apresentar o mesmo comportamento quando aplicadas ao problema de distribuição de chaves secretas.

Entre os formatos de constelação que se aproximam do desempenho da modulação gaussiana ideal, a sinalização não equiprovável dos símbolos QAM (formatação probabilística) é imprescindível para maximizar o desempenho do sistema. Para esquemas de modulação com $N \leq 23^2$ pontos, a distribuição de Maxwell-Boltzmann (gaussiana discreta) com parâmetro ν otimizado apresenta os melhores resultados,

seguida pela distribuição binomial da constelação RW. Ambas são aplicadas à distribuição uniforme de símbolos QAM. No entanto, observou-se que, para $N > 23^2$ pontos, o formato de constelação GQ supera os demais ao utilizar formatação probabilística e geométrica, em que a grade de pontos tem uma distribuição irregular no plano complexo.

No entanto, as constelações formatadas levantam alguns problemas de ordem prática e de segurança quando utilizadas em protocolos QKD. Em relação à formatação geométrica, Cho e Winzer afirmam em [73] que (i) não há solução simples para encontrar a localização dos pontos da constelação para canais arbitrários, (ii) o formato irregular da constelação aumenta a complexidade do processamento digital para recuperação do pulso coerente e (iii) existe uma dificuldade em mapear os símbolos de acordo com um código Gray, aumentando a complexidade do receptor, especialmente para métricas de decisão suave. No caso da formatação geométrica, os pontos são otimizados para maximizar a informação mútua para o canal por meio de algoritmos iterativos, mas não exigem uma arquitetura especial para serem implementados [27]. Os problemas (i) e (iii) referem-se, respectivamente, à complexidade do algoritmo de busca pela distribuição geométrica dos pontos e à dificuldade de usar um código de Gray em constelações com formato radial, que é uma solução comum para constelações com formatação geométrica.

Os problemas encontrados na formatação geométrica são evitados na formatação probabilística. Em geral, (i) a distribuição de probabilidade depende apenas de um parâmetro a ser otimizado, (ii) os pontos da constelação são alocados no plano complexo de acordo com uma modulação QAM convencional, facilitando a recuperação do pulso coerente por meio do processamento digital do sinal especializado para sistemas QAM, e (iii) o mapeamento Gray é aplicado diretamente e é compatível com a decisão suave. Portanto, dos resultados apresentados no Capítulo 3, a formatação probabilística deve ser utilizada com a distribuição gaussiana discreta, a fim de evitar problemas decorrentes de uma constelação com geometria irregular.

No entanto, a utilização de formatação probabilística em QKD tem consequências para a segurança do protocolo. A formatação probabilística é realizada por meio da arquitetura de formatação probabilística de amplitude (PAS) [74], exemplificada na Figura 17, cujo bloco principal é o casador de distribuição (DM, do inglês: *Distribution Matcher*), responsável por converter sequências de símbolos equiprováveis em sequências de símbolos com distribuição arbitrária [74], seguido do codificador de canal (FEC, do inglês: *Forward Error Correction*), que deve ser dispensado em aplicações de QKD[1]. A operação de casamento de distribuição impõe restrições nas possíveis sequências de

[1]Uma vez que a reconciliação reversa é necessária para distâncias com $\tau < 0.5$, cabe a Alice recuperar a sequência de Bob.

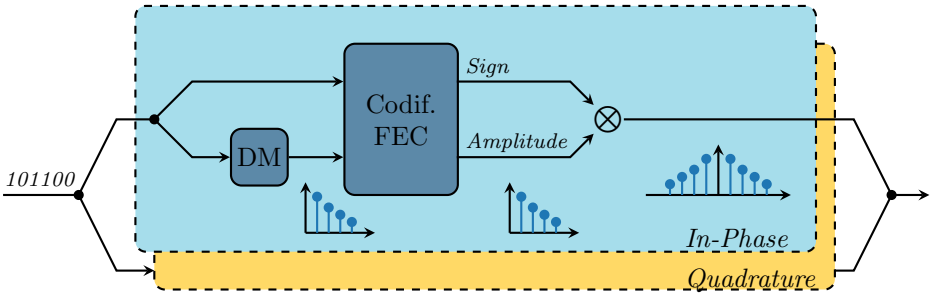


Figura 17 – Arquitetura PCS/PAS.

símbolos de saída do codificador, resultando em correlações entre os símbolos transmitidos e comprometendo a possibilidade de prova de segurança incondicional do protocolo contra ataques arbitrários, uma vez que não apresenta invariância a permutações aleatórias dos estados compartilhados. A invariância à permutação é um dos tipos de simetria que pode ser explorado na redução da segurança de ataques arbitrários para ataques coletivos, sendo importante para a demonstração de algumas variações do teorema quântico de de Finetti [75, 76, 42].

No modelo usual dos protocolos CVQKD (com modulação discreta ou gaussiana), exemplificado na Figura 18a, Alice prepara estados coerentes cujas amplitudes são sorteadas de acordo com uma variável aleatória com um alfabeto complexo. As sequências de amplitudes sorteadas são então utilizadas para construir uma sequência binária com *bits* equiprováveis e independentes, de modo que, se $\boldsymbol{A}, \boldsymbol{B} \in \mathbb{C}^L$ representam as sequências de amplitudes transmitidas por Alice e recuperadas por Bob, respectivamente, $\mathcal{T} : \mathbb{C}^L \times \mathbb{C}^L \to \{0,1\}^l$ é o mapa que representa a ação dos protocolos de correção de erros e amplificação de privacidade, em que $\mathcal{T}(\boldsymbol{A}, \boldsymbol{B})$ é a chave final. Espera-se que $\mathcal{T}(\boldsymbol{A}, \boldsymbol{B}) = \mathcal{T}(\pi(\boldsymbol{A}), \pi(\boldsymbol{B}))$, em que π é um elemento aleatório do grupo de permutação. De forma mais simples, como argumentado em [55], para fins práticos, basta que o protocolo não utilize informações sobre os rótulos dos subsistemas ou sobre a sequência específica de estados para produzir a chave final.

Para sistemas CVQKD com modulação gaussiana de estados coerentes, os protocolos de reconciliação SEC e MD [18, 77], por exemplo, permitem obter as sequências binárias de Alice e Bob, sendo invariantes a permutações. Quando o paradigma é alterado para modulação discreta, não há um método consolidado na literatura para obter as chaves brutas de maneira análoga aos protocolos com modulação gaussiana, com exceção dos protocolos definidos sobre constelações do tipo QPSK, como em [49, 48], nos quais os autores apresentam métodos específicos para Alice e Bob obterem suas respectivas chaves brutas[2]. Portanto, duas abordagens podem

[2]No caso de modulações QPSK, assim como em qualquer esquema de modulação equiprovável, não há preocupação com correlações devido ao casamento de distribuições, e também é possível realizar um

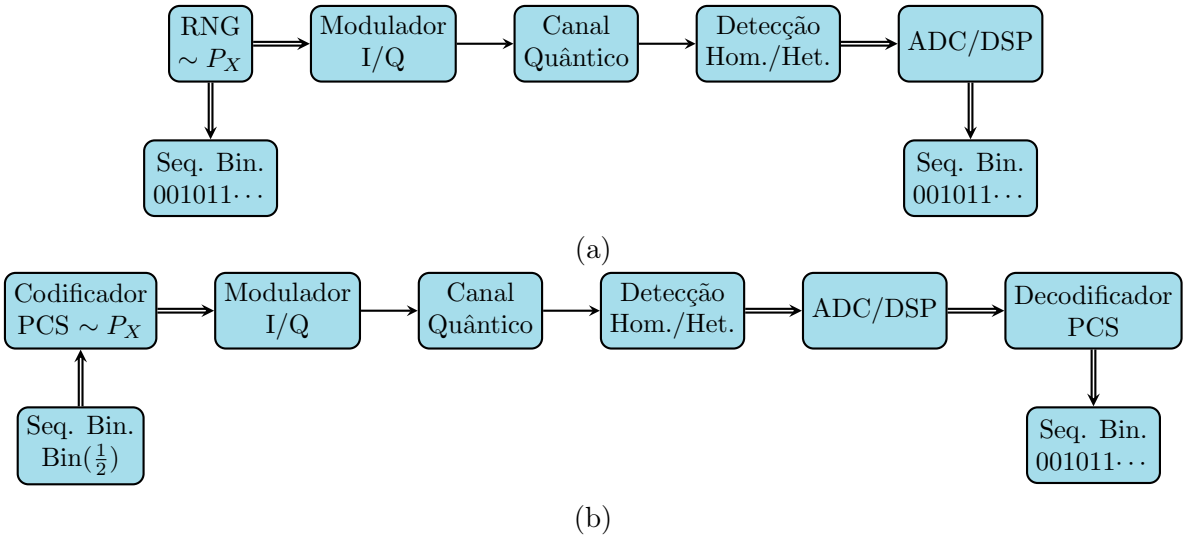


Figura 18 – Esquema geral de um sistema QKD

ser adotadas para resolver o impasse. A primeira seria adaptar a arquitetura PCS/PAS para que ela não gere correlações entre os símbolos de saída e seja invariante a permutações. Dessa forma, como exemplificado na Figura 18b, os estados modulados e enviados pelo canal dependem da estrutura do sistema PCS modificado, bem como da sequência binária gerada aleatoriamente. A segunda abordagem para lidar com o problema é propor uma metodologia para obter sequências binárias aleatórias a partir das sequências de estados transmitidas, mantendo a arquitetura exemplificada na Figura 18a. Vale ressaltar que a arquitetura PCS/PAS não inviabiliza o protocolo, mas impossibilita a redução de ataques arbitrários para coletivos por meio de argumentos baseados na invariância do protocolo a permutações dos subsistemas.

4.2 Reconciliação por Transformada Distributiva[3]

A seção anterior teve como objetivo apresentar os problemas teóricos e práticos na integração de arquiteturas PCS/PAS em sistemas CVQKD com modulação discreta. Nesta seção, será apresentado um método para obter sequências binárias com *bits* independentes e equiprováveis a partir de realizações de variáveis aleatórias. A análise inicial é aplicada a protocolos com modulação gaussiana contínua.

mapeamento simples entre sequências binárias e símbolos da constelação utilizando codificação Gray usual.

[3]Os resultados apresentados nesta Seção foram submetidos para publicação no *Journal of Informtion and Communication Systems* com pre-print disponível em [78]

4.2.1 Expansão por Transformada Distributiva

Os protocolos de reconciliação de informações têm como objetivo garantir que as chaves compartilhadas por Alice e Bob sejam idênticas ao final de sua execução, com alta probabilidade. Uma vez que o resultado da detecção dos estados coerentes são valores reais (ou entendidos como elementos de $\mathbb{R}^2$, no caso de detecção heteródina), a chave bruta deve ser quantizada e as sequências de *bits* resultantes dão origem a canais clássicos virtuais que modelam as correlações entre as sequências binárias de Alice e Bob.

Os protocolos SEC e MD são conhecidos por viabilizar a reconciliação em protocolos com modulação gaussiana, apresentando maneiras de extrair sequências de bits para que um código de correção de erros possa ser aplicado, normalmente um código LDPC [79, 80, 20, 81]. O protocolo SEC realiza partições na reta real (lado de Alice) para atribuir sequências de *bits* a cada intervalo, e estimadores são projetados para recuperar tais sequências no lado de Bob. As sequências resultantes são tratadas como o resultado da transmissão por meio de um canal simétrico binário. A reconciliação MD executa rotações de forma que os valores rotacionados "parecem" ser o resultado da transmissão de sequências de *bits* por meio de um canal AWGN, configurando o canal BIAWGN (do inglês: *Binary Input* AWGN).

Uma alternativa relativamente recente, proposta por Araújo e Assis, apresenta uma abordagem diferente [22]. Baseia-se em dois resultados fundamentais da teoria da informação e da teoria das cópulas, que podem ser usados para extrair sequências de bits independentes de números situados no intervalo unitário. A ideia principal é que os *bits* da expansão binária de uma variável aleatória com distribuição uniforme no intervalo unitário são equiprováveis e independentes. No restante desse capítulo, funções densidade de probabilidade e funções de distribuição acumulada serão denotadas por letras minúsculas e maiúsculas, respectivamente (F e f), bem como $\mathbb{I}$ representa o intervalo unitário fechado $[0, 1]$.

Definição 4.1. *Seja $F : \mathbb{R} \to \mathbb{I}$ uma função de distribuição. A função quasi-inversa de F, também conhecido como inversa generalizada, é a função $F^{(-1)} : \mathbb{I} \to \mathbb{R}$ dada por*

$$F^{(-1)} = \inf\{x \in \mathbb{R} : F(x) \geq t\},\ t \in (0, 1], \tag{4.1}$$

onde $F^{(-1)}(0) = \inf\{x \in \mathbb{R} : F(x) > 0\}$.

Teorema 4.2 ([82])**.** *Seja X uma variável aleatória com função de distribuição F_X e $F_X^{(-1)}$ sua quasi-inverso. Então*

1. *Se F é contínua, então $U = F_X(X)$ é uniformemente distribuída em $[0, 1]$.*

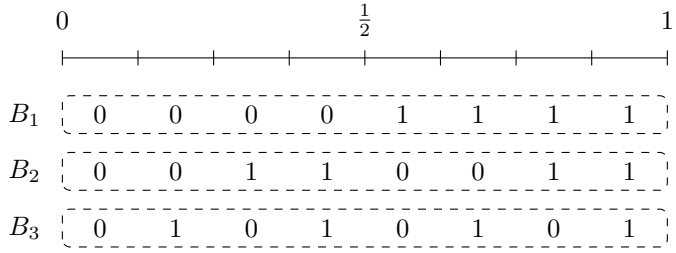


Figura 19 – Particionamento do intervalo unitário com expansão binária de 3 *bits* e os valores correspondentes de cada *bit*.

2. *Se U é uma variável aleatória uniformemente distribuída em $[0,1]$, então $Y = F_X^{(-1)}(U)$ tem uma função de distribuição de acordo com F_X.*

A transformação mencionada na primeira parte do Teorema 4.2 é conhecida como Transformada Distributiva e garante que a transformação de uma variável aleatória por sua função de distribuição contínua sempre leva a uma distribuição uniforme no intervalo unitário. Juntamente com o fato de que os *bits* na expansão binária de uma variável aleatória com distribuição uniforme em $[0,1]$ são independentes e Bernoulli($\frac{1}{2}$) [65], é possível usar a transformada distributiva para mapear os valores da chave bruta no intervalo unitário e aplicar a expansão binária ao valor resultante.

O número $d \in [0,1]$ pode ser expandido na base binária com uma precisão de l *bits* de acordo com a seguinte regra,

$$d \mapsto 0.b_1 b_2 \cdots b_l, \qquad \sum_{i=1}^{l-1} b_i \frac{1}{2^i} \leq d \leq \sum_{i=1}^{l-1} b_i \frac{1}{2^i} + \frac{1}{2^l}, \tag{4.2}$$

e chamamos de $\boldsymbol{b} = b_1 b_2 \cdots b_l$ a sequência de *bits* correspondente. Cada *bit* contém informações sobre onde o número real d está no intervalo unitário: o primeiro *bit* (b_1) informa se $d \in [0, \frac{1}{2})$ ou $d \in [\frac{1}{2}, 1]$, o segundo (b_2) informa se d está na primeira ou segunda metade do intervalo indicado por b_1, ou seja, se $d \in [0, \frac{1}{4})$ ou $d \in [\frac{1}{4}, \frac{1}{2}]$ dado $b_1 = 0$ ou $b_1 = 1$, respectivamente, e assim por diante. Na Figura 19, são representados os valores dos *bits* para cada intervalo em uma expansão de 3 *bits*.

Esse procedimento para extrair *bits* equiprováveis e independentes de realizações de uma variável aleatória contínua X pode ser formalizado como o que chamamos de expansão por transformada distributiva de X (DTE, do inglês: *Distributional Transform Expansion*).

Definição 4.3. *Seja X uma variável aleatória com uma função de distribuição contínua F_X e $\mathcal{Q} : [0,1] \mapsto \{0,1\}^l$ a função que representa a expansão binária da Equação* (4.2)*. A Expansão por Transformada Distributiva (DTE) é definida como*

$$\mathcal{D}(X) = \mathcal{Q}(F_X(X)). \tag{4.3}$$

Uma vez que os bits na expansão binária são independentes, é possível fatorar $\mathcal{D}(X) = \mathcal{D}_1(X)\cdots\mathcal{D}_l(X)$*, onde* $\mathcal{D}_i(X) = \mathcal{Q}_i(F_X(X))$ *é a função* $\mathcal{Q}_i : [0,1] \mapsto \{0,1\}$ *que calcula o i-ésimo bit em Equação* (4.2) *com a propriedade* $\mathcal{D}_i(X) \sim \text{Bern}(\frac{1}{2})$ *. Chamamos de l-*$\mathcal{D}(X)$ *a DTE de X com comprimento l.*

Alice e Bob podem usar a DTE para produzir sequências binárias a partir de seus dados com valores contínuos:

1. Alice e Bob têm as sequências de variáveis gaussianas $X = X_1, \cdots, X_n$ e $Y = Y_1, \cdots, Y_n$ após comunicação quântica e estimação de parâmetros;

2. Alice [Bob in RR] calcula $\mathcal{D}(X) = (\mathcal{D}_1(X), \cdots, \mathcal{D}_l(X))^T$ para cada valor da chave bruta [$\mathcal{D}(Y) = (\mathcal{D}_1(Y), \cdots, \mathcal{D}_l(Y))^T$, em RR]. As sequências de bits resultantes podem ser expressas como matrizes,

$$X \mapsto \begin{bmatrix} \mathcal{D}_1(X_1) & \cdots & \mathcal{D}_1(X_2) \\ \mathcal{D}_2(X_1) & \cdots & \mathcal{D}_2(X_2) \\ \vdots & & \vdots \\ \mathcal{D}_l(X_1) & \cdots & \mathcal{D}_l(X_2) \end{bmatrix} = \begin{bmatrix} \mathcal{D}_1(X) \\ \mathcal{D}_l(X) \\ \vdots \\ \mathcal{D}_l(X) \end{bmatrix}, \tag{4.4}$$

$$Y \mapsto \begin{bmatrix} \mathcal{D}_1(Y_1) & \cdots & \mathcal{D}_1(Y_2) \\ \mathcal{D}_2(Y_1) & \cdots & \mathcal{D}_2(Y_2) \\ \vdots & & \vdots \\ \mathcal{D}_l(Y_1) & \cdots & \mathcal{D}_l(Y_2) \end{bmatrix} = \begin{bmatrix} \mathcal{D}_1(Y) & \\ \mathcal{D}_l(Y) & \vdots \\ \mathcal{D}_l(Y) & \end{bmatrix}, \tag{4.5}$$

3. Cada um dos l pares de sequências $(\mathcal{D}_i(X), Y)$ [$(\mathcal{D}_i(Y), X)$ em RR] pode ser interpretado como um canal AWGN de entrada binária e Bob [Alice in RR] pode recuperar as sequências binárias de Alice [Bob in RR] usando um código de correção de erros.

Exemplo 4.4. *Seja* $X \sim \mathcal{N}(0,1)$*,* $Z \sim \mathcal{N}(0, 0.5)$ *com* $X \perp Z$ *e* $Y = X + Z$*. Assuma as realizações* $x = \{0,491, 0,327, -0,652, -1,096, -0,023\}$ *e* $z = \{-0,722, 0,942, 0,191, 0,198, -0,370\}$*. Então,*

$$F_X(x) = (0.688, 0.628, 0.257, 0.136, 0.491)$$

$$\mapsto \begin{bmatrix} 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

$$F_Y(y) = (0.425, 0.850, 0.353, 0.231, 0.374)$$
$$\mapsto \begin{bmatrix} 0 & 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 \end{bmatrix}.$$

Como os *bits* na expansão são independentes, também é possível que Alice e Bob executem o DTE em suas sequências e tratem os erros entre $\mathcal{D}_i(X)$ e $\mathcal{D}_i(Y)$ conforme transmitido por um canal simétrico binário (BSC) com probabilidade de transição p_i. Essa abordagem foi usada em [22], onde eles mostraram que a reconciliação pode ser obtida nos dois primeiros subcanais com códigos LDPC de tamanho $4 \cdot 10^4$ em no máximo 40 iterações de decodificação com 4.5 dB de snr. No entanto, a análise foi restrita a protocolos CVQKD com detecção homódina, e a eficiência de reconciliação não foi abordada.

Essas duas abordagens possíveis, correção de erros nos canais induzidos BSC e BIAWGN, são as que aparecem intuitivamente após a execução do DTE nas sequências de chaves brutas X e Y. Claramente, a abordagem BSC não deve ter um desempenho melhor do que BIAWGN devido à desigualdade de processamento de dados, que garante que $I(\mathcal{D}_i(X); Y) \geq I(\mathcal{D}_i(X), \mathcal{D}_i(Y))$. A próxima seção se concentrará na caracterização desses dois tipos de subcanais e no desenvolvimento de um limite superior para a eficiência da reconciliação.

4.2.2 Capacidade dos Subcanais DTE

Uma vez que Alice e Bob podem usar a DTE para extrair sequências binárias das chaves brutas de valores contínuos e essas sequências binárias podem se comportar como o resultado da transmissão por canais BSC ou BIAWGN, dependendo se o DTE é executado apenas em X, Y ou ambos, é necessário estimar suas respectivas capacidades. Isso permitirá obter os limitantes superiores da eficiência de reconciliação em cada cenário. Para os canais BSC's, as probabilidades de transição $p_i = \Pr\{\mathcal{D}_i(X) \neq \mathcal{D}_i(Y)\}$ devem ser estimadas, que é a abordagem em [22]. As capacidades BIAWGN dependem de uma análise um pouco mais detalhada na caracterização do canal para estimar $I(\mathcal{D}_i(X); Y)$ para DR e $I(\mathcal{D}_i(Y); X)$ para RR.

A seguir, o canal AWGN induzido conectando as variáveis aleatórias clássicas X da modulação de Alice e Y das saídas de medição de Bob, cujo ruído aparece em função dos parâmetros do canal quântico. Expressões para eficiência de reconciliação também são dadas para reconciliação direta e reversa.

Canal AWGN Equivalente

Retomando o protocolo com modulação gaussiana e detecção homódina (GG02 [13]), na versão do protocolo EB, o estado compartilhado de Alice e Bob após a transmissão do canal quântico e antes da detecção tem a seguinte matriz de covariância [59],

$$\boldsymbol{\Sigma}'_{AB} = \begin{pmatrix} V\boldsymbol{I}_2 & \sqrt{\tau}\sqrt{V^2-1}\boldsymbol{Z} \\ \sqrt{\tau}\sqrt{V^2-1}\boldsymbol{Z} & [\tau V_m + 1 + \xi]\boldsymbol{I}_2 \end{pmatrix}, \tag{4.6}$$

onde $V = V(\hat{q}) = V(\hat{p}) = V_m + 1$ é a variância total da quadratura, $V_m = 4\tilde{V}_m$ e $\xi = 2\bar{n}(1-\tau)$ é o ruído de excesso do canal, sendo $\varepsilon = 2\bar{n} + 1$ o ruído térmico do canal e $\bar{n}$ indicando o número médio fótons térmicos excitados no modo. O modo de Bob está em um estado térmico com primeiro momento centrado na origem e com matriz de covariância $\boldsymbol{\Sigma}'_B = [\tau V_m + 1 + \xi]\boldsymbol{I}_2$, e para a detecção homódina, a distribuição de probabilidade dos resultados das medições será [83],

$$p_Y(y) = \sqrt{\frac{1}{2\pi\sigma_Y^2}}\exp\left(-\frac{1}{2}\frac{y^2}{\sigma_Y^2}\right), \tag{4.7}$$

sendo $\sigma_Y^2 = (\tau V_m + \xi + 1)/4$. Lembrando que $X \sim \mathcal{N}(0, \tilde{V}_m)$, é possível reescrever $Y = \sqrt{\tau}X + Z'$, com $Z' \sim \mathcal{N}\big(0, \frac{\xi+1}{4}\big)$ e $X \perp Z$. Aplicando uma normalização, obtemos o modelo de canal AWGN $Y = X + Z$, com $Z'/\sqrt{\tau} = Z \sim \mathcal{N}(0, \sigma_{Z_1}^2 = (\xi+1)/4\tau)$ e $\sigma_Y^2 = \tilde{V}_m + \frac{\xi+1}{4\tau}$. A relação-sinal-ruído é dada então por

$$\mathsf{snr}_{hom} = \frac{\tau V_m}{1+\xi}. \tag{4.8}$$

No caso em que a detecção heteródina é utilizada por Bob (*no-switching* [15]), o modo recebido passa por um divisor de feixe balanceado e os modos resultantes são descritos pela matriz de covariância [59],

$$\boldsymbol{\Sigma}'_{B_1B_2} = \begin{pmatrix} \big(\frac{\tau}{2}V_m + 1 + \frac{\xi}{2}\big)\boldsymbol{I}_2 & -\frac{\tau V_m \xi}{2}\boldsymbol{I}_2 \\ \frac{\tau V_m \xi}{2}\boldsymbol{I}_2 & \big(\frac{\tau}{2}V_m + 1 + \frac{\xi}{2}\big)\boldsymbol{I}_2 \end{pmatrix}. \tag{4.9}$$

Esquemas de detecção homódina são aplicados em cada modo de saída do divisor de feixe[4], resultando na mesma distribuição $Y_q \sim Y_p \sim \mathcal{N}(0, \sigma_Y^2 = (\frac{\tau}{2}V_m + 1 + \frac{\xi}{2})/4)$ e podem ser vistos como $Y_* = \sqrt{\tau/2}X + Z'$, sendo $Z' \sim \mathcal{N}(0, \frac{1+\xi/2}{4})$. Como no caso da detecção homódina, é utilizada uma normalização resultando em $Y_* = X + Z$ com $\sqrt{\frac{2}{\tau}}Z' = Z \sim \mathcal{N}(0, \sigma_{Z_2}^2 = \frac{1+\xi/2}{2\tau})$ e $\sigma_Y^2 = \tilde{V}_m + (\xi/2+1)/2\tau$. A relação-sinal-ruído resultante será,

$$\mathsf{snr}_{het} = \frac{\frac{\tau}{2}V_m}{1+\frac{\xi}{2}}. \tag{4.10}$$

[4]Motivo pelo qual o termo "homódina dupla" é utilizado para denotar detecção homódina.

É importante observar que, para detecção homódina ou heteródina, a relação sinal-ruído é função da variância da modulação (conhecida por Alice e Bob antes da execução do protocolo) e das quantidades invariantes do canal[5] (τ e ξ), portanto, dados os valores de $\tilde{V}_m$, τ e ξ, $\mathsf{snr}_{hom} \neq \mathsf{snr}_{het}$. Além disso, devido à simetria na modulação e à independência entre as quadraturas, as eficiências de reconciliação homódina e heteródina podem ser estimadas simplesmente simulando um canal AWGN. Para a medição heteródina, é suficiente estimar apenas uma das quadraturas.

Capacidade dos Sub-canais DTE

As capacidades dos subcanais induzidos pela expansão binária foram estimadas simulando os canais AWGN caracterizados na seção anterior. Inicialmente, foram estimadas as capacidades dos subcanais do BSC estimando as probabilidades de transição $p_i = \Pr\{\mathcal{D}_i(X) \neq \mathcal{D}_i(Y)\}$. Para os canais BIAWGN, foram utilizados os estimadores de entropia disponíveis em [84], que implementam o estimador de informação mútua [85] para obter $I(\mathcal{D}_i(X);Y)$ e $I(\mathcal{D}_i(Y);X)$. Os resultados estão apresentados nas Figuras 20 e 21. É possível observar que, à medida que mais *bits* são extraídos das variáveis X e Y, os subcanais resultantes tornam-se mais ruidosos, aproximando-se rapidamente do comportamento de uma moeda honesta, como ilustrado na Figura 20. Vale ressaltar que as probabilidades de transição do BSC são independentes da direção de reconciliação, assim como as capacidades.

A Figura 21 apresenta as capacidades dos subcanais para BIAWGN e BSC para RR e DR com detecção heteródina e homódina. É observado que as capacidades dos canais BSC (linhas tracejadas) estão bastante distantes das capacidades dos canais BIAWGN (linhas sólidas), o que nos leva à conclusão de que aplicar o DTE nas sequências de Alice e Bob não resultará em uma boa eficiência de reconciliação. As capacidades correspondentes dos canais BIAWGN quando a reconciliação direta é considerada também são plotadas, mostrando-se muito próximas à reconciliação reversa. Embora a reconciliação direta esteja restrita a $\tau > 0,5$, e como será visto na próxima seção, a melhor eficiência do DTE é encontrada na região com $\mathsf{snr}< 0$ dB. Portanto, uma análise mais aprofundada sobre a eficiência da reconciliação será restrita à direção de reconciliação reversa.

4.2.3 Eficiência de Reconciliação

O processo de quantização executado pela expansão DTE é uma função $\mathcal{D} : \mathbb{R} \mapsto \{0,1\}^l$ que pode ser fatorada em l funções de quantização $\mathcal{D}_i : \mathbb{R} \mapsto \{0,1\}$, $i = 1, \cdots, l$,

[5] O modelo utilizado para o canal quântico admite que os parâmetros de transmitância e ruído térmico/excesso são fixos durante toda a comunicação.

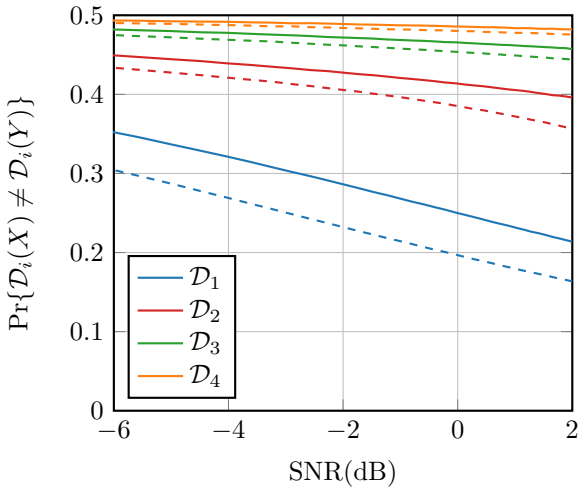
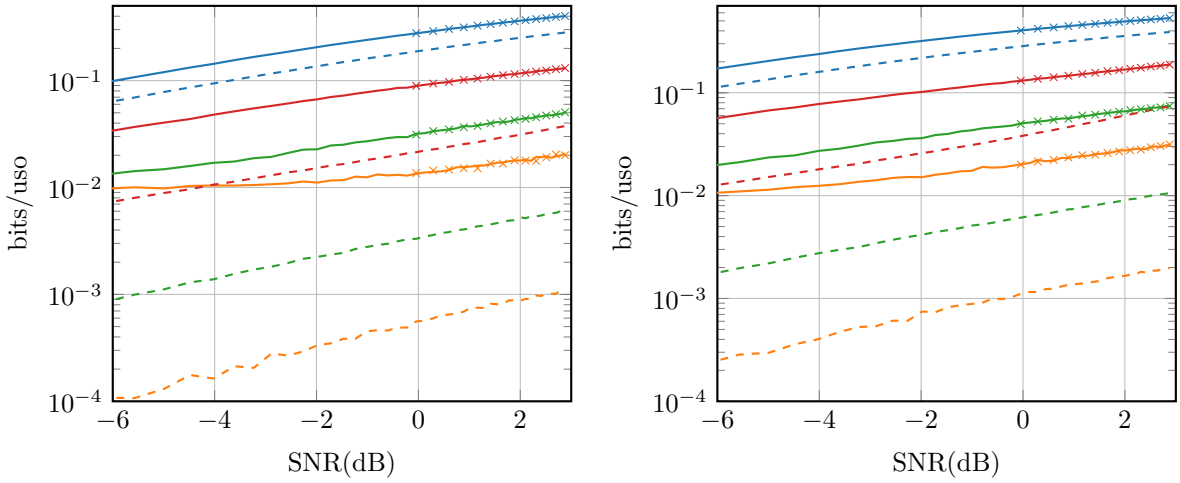


Figura 20 – Probabilidade de transição $\Pr\{\mathcal{D}_i(X) \neq \mathcal{D}_i(Y)\}$ dos subcanais BSC induzidos pela expansão DTE de quatro *bits*. As probabilidades foram estimadas pela realização de $N = 10^4$ sorteios da variável aleatória de Alice e repetindo o experimento 10^3 vezes. Os parâmetros foram $\tilde{V}_m = 1$ e $\xi = 0.02$ tanto para detecção de heteródina (linhas sólidas) quanto homódina (linha tracejada).



(a) Heteródina. (b) Homódina.

Figura 21 – Capacidades de subcanais do BIAWGN e BSC induzidos pela expansão DTE em um protocolo CVQKD modulado gaussiana e detecção heteródina/homódina considerando os casos de reconciliação direta e reversa. A capacidade foi estimada pela experimento aleatório de $N = 10^4$ realizações da variável aleatória de Alice e estimando a informação mútua $I(\mathcal{D}_i(Y); X)$ (linhas sólidas) e $I(\mathcal{D}_i(X); Y)$ para BIAWGN, e calculando $C_{BSC_i} = 1 - H(p_i)$ para BSC (linhas tracejadas), onde p_i é a probabilidade de transição estimada mostrada em Figura 20. Os experimentos foram repetidos 10^3 vezes para ambos os métodos de detecção e os resultados apresentados são os valores médios. Nos gráficos, $\mathcal{D}_1$ está na parte superior e $\mathcal{D}_4$ na parte inferior.

conforme indicado na Definição 4.3. Aqui, serão derivadas as expressões gerais para as eficiências de reconciliação alcançáveis ao usar a expansão DTE para sequências binárias. A seguir, usaremos as setas direita e esquerda para indicar as direções de reconciliação direta e reversa, respectivamente.

Reconciliação Direta

Primeiro, considere que Alice aplica a DTE às n realizações de suas variáveis gaussianas X, de forma que Bob deve recuperar sua sequência binária. A taxa secreta *por estado transmitido* na reconciliação direta (DR) é dada por [86],

$$K^{\rightarrow} = H(\mathcal{D}(X)) - \chi(X,E) - l^{-1}|M^{\rightarrow}|, \tag{4.11}$$

$$= \beta^{\rightarrow} I(X;Y) - \chi(X,E), \tag{4.12}$$

$|M^{\rightarrow}|$ a quantidade de informação lateral que Alice deve enviar para Bob na reconciliação direta, e

$$\beta^{\rightarrow} = \frac{H(\mathcal{D}(X)) - l^{-1}|M^{\rightarrow}|}{I(X;Y)}. \tag{4.13}$$

O limite superior da eficiência de reconciliação é alcançado quando Alice usa a quantidade mínima de informação lateral, ou seja, quando $|M| \cdot l^{-1} = H(\mathcal{D}(X)|Y)$, e a máxima eficiência de reconciliação será

$$\beta^{\rightarrow}_{max} = \frac{H(\mathcal{D}(X)) - H(\mathcal{D}(X)|Y)}{I(X;Y)} \geq \beta^{\rightarrow}. \tag{4.14}$$

Desenvolvendo a entropia condicional em Equação (4.14),

$$H(\mathcal{D}(X)|Y) \overset{(a)}{=} H(\mathcal{D}_1(X), \cdots, \mathcal{D}_l(X)|Y), \tag{4.15}$$

$$\overset{(b)}{=} H(\mathcal{D}_1(X)|Y) + H(\mathcal{D}_2(X)|\mathcal{D}_1(X), Y) +$$

$$\cdots + H(\mathcal{D}_l(X)|\mathcal{D}_{l-1}(X), \cdots, \mathcal{D}_1(X), Y) \tag{4.16}$$

$$\overset{(c)}{=} \sum_{i=1}^{l} H(\mathcal{D}_i(X)|Y) \tag{4.17}$$

$$\overset{(d)}{=} \sum_{i=1}^{l} \left(H(\mathcal{D}_i(X)) - I(\mathcal{D}_i(X);Y)\right) \tag{4.18}$$

$$\overset{(e)}{=} l - \sum_{i=1}^{l} I(\mathcal{D}_i(X);Y), \tag{4.19}$$

onde (a) vem de Definição 4.3, (b) é a regra da cadeia para a entropia conjunta, (c) é devido a $\mathcal{D}_i(X) \perp \mathcal{D}_j(X), i \neq j$, (d) vem da identidade $H(A|B) = H(A) - I(A;B)$ e (e)

segue de $\mathcal{D}_i(X) \sim \text{Bern}(\frac{1}{2})$, que dá $H(\mathcal{D}_i(X)) = 1$. Conclui-se que

$$\beta^{\rightarrow}_{max} = \frac{H(\mathcal{D}(X)) - l + \sum_{i=1}^{l} I(\mathcal{D}_i(X); Y)}{I(X;Y)}, \tag{4.20}$$

$$= \frac{\sum_{i=1}^{l} I(\mathcal{D}_i(X); Y)}{I(X;Y)}, \tag{4.21}$$

uma vez que $H(\mathcal{D}(X)) = H(\mathcal{D}_1(X), \cdots, \mathcal{D}_l(X)) = H(\mathcal{D}_1(X)) + \cdots + H(\mathcal{D}_l(X)) = l$. Ou seja, a eficiência máxima é proporcional à fração de informação mútua nos subcanais que o DTE consegue extrair do canal AWGN real.

Reconciliação Reversa

Na reconciliação reversa, Bob realiza a expansão DTE em sua sequência Y e deve enviar informações laterais para que Alice faça a correção de erros. Dessa maneira, a taxa de chave secreta *por estado transmitido* na reconciliação reversa torna-se

$$K^{\leftarrow} = H(\mathcal{D}(Y)) - \chi(Y, E) - l^{-1}|M^{\leftarrow}|, \tag{4.22}$$

$$= \beta^{\leftarrow} I(X;Y) - \chi(Y, E), \tag{4.23}$$

e, analogamente ao caso da reconciliação direta, $|M^{\leftarrow}|$ é a quantidade de informações que Bob deve enviar para Alice, e

$$\beta^{\leftarrow} = \frac{H(\mathcal{D}(Y)) - l^{-1}|M^{\leftarrow}|}{I(X;Y)}. \tag{4.24}$$

Seguindo o mesmo procedimento de reconciliação direta, quando $l^{-1}|M^{\leftarrow}| \rightarrow H(\mathcal{D}(Y)|X)$, a eficiência de reconciliação máxima na direção reversa é dada por

$$\beta^{\leftarrow} \leq \beta^{\leftarrow}_{max} = \frac{H(\mathcal{D}(Y)) - H(\mathcal{D}(Y)|X)}{I(X;Y)},$$

$$= \frac{\sum_{i=1}^{l} I(\mathcal{D}_i(Y); X)}{I(X;Y)}. \tag{4.25}$$

Discussão Sobre a Eficiência de Reconciliação

Antes de mais nada, é necessário destacar que, tanto na reconciliação direta quanto na reconciliação reversa, trocar a quantidade mínima de informações laterais implica que os códigos de correção de erros devem ser executados na capacidade dos canais, e este é o único fator que afeta a eficiência do protocolo de reconciliação usando DTE. A expressão na Equação (4.20) é a mesma que em outros métodos de reconciliação de informações usando a SEC [62]. Porém, a entropia[6] $H(\mathcal{Q}(X))$ no protocolo SEC não é necessariamente

[6]Neste parágrafo usamos $\mathcal{Q}$ como uma função de quantização genérica.

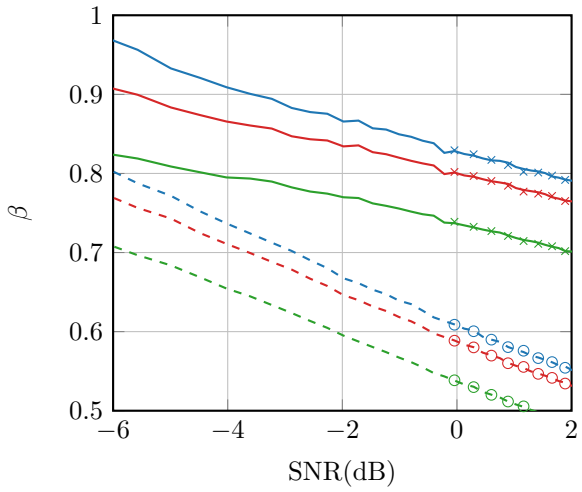


Figura 22 – Eficiência de reconciliação alcançada pela l-DTE de cordo com as Equações (4.21) e (4.25), com $l \in \{2, 3, 4\}$ (curvas em verde, vermelho e azul, respectivamente), $\tilde{V}_m = 1$ e $\xi = 0.02$. As linhas sólidas e tracejadas correspondem às eficiências para detecção homódina e heteródina, respectivamente.

igual a $|\mathcal{Q}(X)|$, e tal igualdade vem naturalmente no DTE devido à independência dos *bits* na expansão.

Traçamos as curvas para a eficiência de reconciliação das Equações (4.21) e (4.25) na Figura 22 para detecções heteródinas e homódinas com $\tilde{V}_m = 1$, $\xi = 0,02$, e considerando $l \in 2, 3, 4$ sequências de *bits* extraídas (correspondente às curvas em preto, vermelho e azul, respectivamente). Há alguns pontos interessantes a serem destacados. Um deles é que uma reconciliação baseada na DTE parece ter o mesmo desempenho para RR e DR (no intervalo aplicável de snrpara ambas as direções), o que pode implicar simetria: $I(\mathcal{D}_i(X); Y) = I(\mathcal{D}_i(Y); X)$.

Em segundo lugar, a máxima eficiência de reconciliação aparece como uma função decrescente da snr. Embora o DTE não tenha um bom desempenho com protocolos CVQKD baseados em detecção homódina, as curvas referentes às simulações com medições heteródinas apresentam resultados promissores. Neste caso, uma expansão de três bits resulta em $\beta^{\leftarrow}_{\max} > 0.8$ para snr < 0 dB e $\beta^{\leftarrow}_{\max} > 0.9$ para snr < -3.6 dB. Aqui, outra diferença operacional aparece entre SEC e DTE. No protocolo SEC, comumente são divulgados os subcanais com informação mútua inferior a 0,02 bits (geralmente os dois primeiros bits da sequência), enquanto no DTE, até mesmo o quarto subcanal, que apresenta informação mútua em torno de 0,01 bits para snr < -3.6 dB, é crucial para que a eficiência de reconciliação seja maior que 0,9. Os subcanais BIAWGN induzidos por DTE com snr > -2 dB têm os três primeiros bits acima do limite de 0,02 *bit* comumente adotado para o protocolo SEC.

A diferença na eficiência da reconciliação DTE com detecções homódinas e heteródinas também é notável; para discutir isso, consideramos o caso de reconciliação reversa. Para a detecção homódina, Alice e Bob possuem variáveis aleatórias gaussianas X e Y correlacionadas e, assim, em Equação (4.25), $I(X;Y) = \log(1+\mathsf{snr}_{\mathrm{hom}})/2$, o que resulta em

$$\beta_{max}^{hom} = \frac{H(\mathcal{D}(Y)) - l + \sum_{i=1}^{l} I(\mathcal{D}_i(Y);X)}{\log(1+\mathsf{snr}_{hom})/2}. \tag{4.26}$$

Quando a detecção heteródina é usada, as quadraturas são detectadas simultaneamente, resultando em $2l$ sequências binárias extraídas usando DET, l para cada quadratura. Devido às simetrias, os i-ésimos subcanais das quadraturas q e p são estatisticamente idênticos. Então,

$$\beta_{max}^{het} = 2 \cdot \frac{H(\mathcal{D}(Y)) - l + \sum_{i=1}^{l} I(\mathcal{D}_i(Y);X)}{\log(1+\mathsf{snr}_{het})}. \tag{4.27}$$

Formatação e Segurança

Neste capítulo, foi discutido como as etapas de processamento da informação clássica podem afetar as propriedades de simetria do protocolo de distribuição de chaves e como a arquitetura usual de formatação probabilística de constelações é inerentemente dependente da sequência dos estados transmitidos. Uma das maneiras de resolver essa dependência é a proposta de um protocolo de reconciliação que realiza a extração de sequências de *bits iid* de uma fonte que emite símbolos não equiprováveis, de modo que o protocolo mantenha a invariância a permutações e compatibilidade com a estrutura de prova de segurança utilizada para os protocolos com modulação gaussiana contínua. No próximo capítulo, iniciaremos a discussão sobre a análise de segurança de protocolos CVQKD com modulação discreta.

Parte III

Segurança

Capítulo 5

Perspectivas sobre a Análise de Segurança

Este capítulo inicia a discussão sobre a análise de segurança de protocolos CVQKD com modulação não gaussiana. Nos capítulos anteriores, foram apresentados a estrutura geral de um protocolo QKD – preparação e detecção de estados quânticos, tipo de ataque físico realizado pela espiã (clonagem por emaranhamento), e as estratégias para obtenção de informação secreta pela interação com os estados transmitidos durante a execução do protocolo (ataques individuais, coletivos e coerentes). O desempenho dos protocolos com modulação discreta foi avaliado levando em consideração ataques coletivos e, para calcular o limitante superior da informação acessível da espiã, foi utilizado o argumento do estado gaussiano equivalente, em que Alice e Bob utilizam as medidas de informação calculadas a partir do estado gaussiano com matriz de covariância idêntica à reconstruída do protocolo PM com modulação não gaussiana. Chamaremos essa manobra de hipótese gaussiana.

Nas próximas seções, serão discutidos os efeitos do uso dessa hipótese no cálculo da taxa de chave secreta. A discussão será iniciada na Seção 5.1 e na Seção 5.2 será apresentada uma proposta de análise do ataque de clonagem por emaranhamento. A análise do "erro de aproximação" causado pela hipótese gaussiana será abordada no Capítulo 6, bem como alguns aspectos sobre a segurança incondicional do protocolo.

5.1 Ataques coletivos, Clonagem por Emaranhamento e a Hipótese Gaussiana

A ideia básica de um protocolo QKD é viabilizar a geração chaves aleatórias com segurança incondicional compartilhadas por duas partes geograficamente distantes, e por segurança incondicional entendemos que a espiã Eva não terá informação a respeito da

mensagem cifrada com o uso da chave gerada a despeito de sua capacidade computacional [8]. Não limitar as capacidades da espiã significa que ela só está submetida às limitações da natureza, a saber, da mecânica quântica, e, a partir das chaves brutas compartilhadas, Alice e Bob devem estimar o que a espiã pode ter aprendido durante a comunicação quântica.

Entretanto, analisar para quais condições um protocolo pode ser assumido incondicionalmente seguro sem de fato restringir as ações da espiã pode facilmente se tornar uma tarefa complicada e, como foi apresentado na Seção 2.2, Alice e Bob podem analisar a segurança do protocolo sob diferentes hipóteses de ataque de espionagem que resulta em limitantes inferiores para a taxa de chave secreta (desempenho) distintos. Cada hipótese confere diferentes graus de liberdade às capacidades da espiã: tipo de interação com os sistemas de Alice e Bob (ataque físico) e detecção dos seu sistemas (medições individuais ou coletivas) e um protocolo é dito de fato incondicionalmente seguro quando protegido contra ataques coerentes por parte da espiã[1]. A análise de segurança para ataques arbitrários é uma tarefa complicada e a estratégia para estabelecer a segurança do protocolo dá um passo atrás: inicialmente é pressuposto que Eva realiza ataques coletivos e então é feito um esforço para mostrar que a segurança contra ataques coletivos é equivalente (proporcional) à segurança contra ataques arbitrários, a menos de um fator que pode ser feito arbitrariamente pequeno, para o protocolo em questão. Os aspectos de segurança incondicional serão abordados na Seção 6.2.

Então, voltando a atenção para a estratégia de ataques coletivos, temos que este tipo de ataque é compatível com o cenário prático em que Alice e Bob se comunicam por meio de uma fibra ótica modelada como um canal gaussiano linear de um modo (atenuante com ruído térmico), que pode ser simulado pela espiã através do procedimento de clonagem por emaranhamento. Essa compatibilidade se deve ao fato de que canais gaussianos de um modo podem ser tomados como o efeito de ataques coletivos gaussianos realizados pela espiã [58] e ataques gaussianos, isto é, operações unitárias gaussianas realizadas pela espiã, maximizam a informação acessível à espiã [23, 24, 56]. De acordo com [58], a máquina de clonagem por emaranhamento é a descrição mais geral do ataque gaussiano.

Em um protocolo com modulação gaussiana, como o GG02 ou UD-CVQKD apresentados na Seção 2.3, o estado bipartido compartilhado para o protocolo baseado em emaranhamento pode ser completamente descrito pelos dois primeiros momentos estatísticos e, somando ao fato de que Eva deve realizar a mesma estratégia de ataque durante toda a comunicação quântica, i.e., os parâmetros de transmissividade e ruído de

[1] Alguns outros critérios de segurança podem ser discutidos e adicionados à análise, como definições de composibilidade e cenários não assintóticos, por exemplo, os quais não serão tratados por este trabalho.

excesso são mantidos constantes durante os ataques, Alice e Bob podem realizar uma tomografia do canal durante a estimação de parâmetros[2] para obter τ e ξ. De fato, após as N rodadas da fase quântica do protocolo, Alice e Bob compartilham o estado-produto $\hat{\rho}_{AB} = \hat{\sigma}_{AB}^{\otimes N}$, $\hat{\sigma}_{AB} \in \mathcal{D}(\mathcal{H}_A \otimes \mathcal{H}_B)$ com matriz de covariância

$$\mathbf{\Gamma} = \begin{pmatrix} V\boldsymbol{I} & \sqrt{V^2-1}\boldsymbol{Z} \\ \sqrt{V^2-1}\boldsymbol{Z} & V\boldsymbol{I} \end{pmatrix} \xrightarrow{\mathcal{E}_{\tau,\xi}^{th}} \begin{pmatrix} V\boldsymbol{I} & \sqrt{\tau}\sqrt{V^2-1}\boldsymbol{Z} \\ \sqrt{\tau}\sqrt{V^2-1}\boldsymbol{Z} & [\tau(V-1)+1+\xi]\boldsymbol{I} \end{pmatrix} = \mathbf{\Gamma}'. \quad (5.1)$$

Uma vez que o canal térmico não deve imprimir correlações entre as quadraturas de $\hat{\sigma}_{AB}$ e, como em ataques coletivos admite-se que Eva interage individualmente com cada estado, é justificada a forma de $\hat{\rho}_{AB}$ em produto e, consequentemente, terá matriz de covariância[3]

$$\mathbf{\Gamma}'_N = \begin{pmatrix} \mathbf{\Gamma}' & \mathbf{0} & \cdots & \mathbf{0} \\ \mathbf{0} & \mathbf{\Gamma}' & \cdots & \mathbf{0} \\ \vdots & \vdots & \ddots & \vdots \\ \mathbf{0} & \mathbf{0} & \cdots & \mathbf{\Gamma}' \end{pmatrix}. \quad (5.2)$$

Logo, $\hat{\sigma}_{AB}$ é um tipo de estado *protótipo* para o protocolo e permite estimar $\mathbf{\Gamma}$ por meio das observações realizadas em um protocolo do tipo P&M [59]. Para o caso do GG02, Alice e Bob detém as sequências aleatórias $X_N = x_1, \cdots, x_N$ e $Y_N = y_1, \cdots, y_N$, logo,

$$\begin{cases} V & = \langle X^2 \rangle + 1, \\ \tau & = \frac{\langle XY \rangle^2}{\langle X^2 \rangle^2}, \\ \tau(V-1)+1+\xi & = \langle Y^2 \rangle. \end{cases} \quad (5.3)$$

Para protocolos gaussianos, a análise de segurança de um protocolo EB equivalente sob ataque coletivo é uma "via de mão dupla". Do ponto de vista de Eva, o tipo de acoplamento realizado que confere maior quantidade de informação acessível ao estados compartilhados por Alice e Bob é por meio de uma operação unitária gaussiana, a máquina de clonagem por emaranhamento, que simula um canal gaussiano entre Alice e Bob. Já para Alice e Bob, sabendo que no protocolo EB foi utilizado um estado gaussiano e tudo que eles "têm em mãos" são as chaves brutas para estimar o quanto de informação que foi "perdida para o canal" (em última instância, Eva), é seguro estimar os termos da matriz de covariância e assumir que, após o canal quântico, os estados compartilhados são também gaussianos[4] pois é o cenário que maximiza a informação da espiã, o pior caso.

[2] A matriz de covariância de um sistema bipartido tem dimensão 4×4 e é simétrica então, a rigor, seria necessário que a tomografia estimasse seus dez parâmetros para reconstruir o estado compartilhado. Porém, como argumentado em [8, Seção 3.3.5], Alice e Bob podem realizar um procedimento de *simetrização* para que Γ tenha a forma da Equação (5.1).

[3] Note que as formas de $\mathbf{\Gamma}$ e $\mathbf{\Gamma}'_N$, admitindo que o canal não força correlações entre modos ou entre estados, são hipóteses experimentais razoáveis garantidas teoricamente pelos processos de simetrização no espaço de fase, os quais possibilitam que Alice e Bob podem de fato estimar os parâmetros do canal.

[4] Um canal gaussiano mapeia estados gaussianos em estados gaussianos.

Isso é o que chamaremos de *hipótese gaussiana*: Alice e Bob, não podendo realizar uma tomografia completa dos estados compartilhados, estimam os parâmetros do canal sabendo que, para ataques coletivos, o canal gaussiano é o cenário de pior caso. A hipótese gaussiana não é apenas experimentalmente razoável como também teoricamente segura.

Porém, um dilema surge quando consideramos protocolos com modulação não gaussiana (nG). Nos protocolos CVQKD que aplicam modulação discreta com constelação representada pela mistura $\hat{\rho} = \sum_i p_i \hat{\rho}_i$, é possível definir um protocolo EB equivalente, como apresentado em [8, 45, 48, 50], em que, no lugar de um estado TMSV, Alice e Bob compartilham um estado puro bipartido $\hat{\rho}_{AB} = |\Psi\rangle\langle\Psi|_{AB}$ com matriz de covariância[5] $\mathbf{\Gamma}_\Psi$ que é uma purificação de $\hat{\rho}$ e *certamente* não gaussiano. Com certeza $\mathbf{\Gamma}_\Psi$ (juntamente com o primeiro momento) não caracteriza $\hat{\rho}_{AB}$ *completamente* e a entropia de von Neumann $S(\hat{\rho}_{AB})$ não pode ser calculada pelos autovalores simpléticos de $\mathbf{\Gamma}_\Psi$, por exemplo. Contudo, Alice e Bob podem utilizar a hipótese gaussiana e assumir o estado $\hat{\rho}^G_{AB}$ – o estado gaussiano equivalente a $\hat{\rho}_{AB}$ com o mesmo vetor de média e matriz de covariância que $\hat{\rho}_{AB}$, calcular a taxa de chave secreta a partir de $\mathbf{\Gamma}_\Psi$ a qual será um limitante inferior para a taxa de chave secreta do protocolo com modulação nG.

De acordo com a propriedade de extremalidade dos estados gaussianos, Teorema B.21, o limitante inferior para a taxa de chave secreta de um protocolo QKD definido por um estado bipartido $\hat{\rho}_{AB}$ com primeiro e segundo momentos finitos é obtido pelo estado gaussiano equivalente $\hat{\rho}^G_{AB}$ [23]. Entretanto, é razoável questionar o quanto o uso da hipótese gaussiana em protocolos com modulação nG subestima seu desempenho.

Exemplo 5.1. *Tomemos a seguinte mistura equiprovável de estados coerentes* $\hat{\rho} = \frac{1}{2}|\gamma\rangle\langle\gamma| + \frac{1}{2}|-\gamma\rangle\langle-\gamma|$ *em que* $\gamma = \alpha e^{j\pi/4}$. *O estado gaussiano equivalente* $\hat{\rho}^G$ *será definido pela matriz de covariância* $\mathbf{\Gamma} = (2\alpha^2+1)\boldsymbol{I}$ *e* $S(\hat{\rho}^G) = g(\nu)$, *sendo* $\nu = 2\alpha^2+1$ *o autovalor simplético de* $\mathbf{\Gamma}$ *e* $g(\cdot)$ *a função entrópica bosônica. Por outro lado, é possível obter a forma diagonal*[6] $\hat{\rho} = \mu_1|\phi_1\rangle\langle\phi_1| + \mu_1|\phi_2\rangle\langle\phi_2|$, *sendo* $\mu_1 = e^{-\alpha^2}\cosh\alpha^2$, $\mu_2 = e^{-\alpha^2}\sinh\alpha^2$ *e*

$$|\phi_1\rangle = \frac{1}{\sqrt{\cosh\alpha^2}} \sum_{n=0}^{\infty} \frac{(-j)^n \alpha^{2n}}{\sqrt{(2n)!}} |2n\rangle\,, \tag{5.4}$$

$$|\phi_2\rangle = \frac{1}{\sqrt{\sinh\alpha^2}} \sum_{n=0}^{\infty} e^{-j\pi/4} \frac{(-j)^n \alpha^{2n+1}}{\sqrt{(2n+1)!}} |2n+1\rangle\,, \tag{5.5}$$

de modo que $S(\hat{\rho}) = H(\mu)$.

[5]Para constelações simétricas em relação à origem, o primeiro momento é o vetor nulo.

[6]Os estados $|\phi_1\rangle$ e $|\phi_2\rangle$ são os *coherent cat states* $|cat_+\rangle = (|\gamma\rangle + |\gamma\rangle)$ e $|cat_-\rangle = (|\gamma\rangle + |\gamma\rangle)$ com fatores de normalização $\mu_1 = \sqrt{\langle cat_+|cat_+\rangle}$ e $\mu_2 = \sqrt{\langle cat_-|cat_-\rangle}$.

As curvas para $S(\hat{\rho})$ e $S(\hat{\rho}^G)$ estão apresentadas na Figura 23a. É possível notar que os valores de entropia da mistura de estados e do seu equivalente gaussiano são praticamente indistinguíveis na região $\alpha < 0.2$ mas, conforme a energia de $\hat{\rho}$ aumenta, as entropias divergem. Então, a hipótese gaussiana provê uma aproximação segura quando constelações de baixa energia são consideradas e resulta em um limitante inferior próximo do valor real da taxa de chave. Em contrapartida, quando a energia média da mistura de estados aumenta, é possível que o "erro de aproximação" seja notavelmente discrepante.

Ainda mais, se considerarmos o protocolo DM-CVQKD definido pela constelação representada por $\hat{\rho}$, sua taxa de chave secreta pode ser calculada de duas maneira. A primeira é de acordo com os procedimento apresentados no Capítulo 3 com as quantidades de informação entre Alice, Bob e Eva calculadas pelo protocolo P&M. A outra é por um protocolo EB equivalente, em que Alice inicia com o estado bipartido

$$|\Phi_B\rangle_{AB} = \sqrt{\mu_1}\,|\phi_1\rangle\,|\phi_1\rangle + \sqrt{\mu_2}\,|\phi_2\rangle\,|\phi_2\rangle\,, \tag{5.6}$$

que é uma purificação de $\hat{\rho}$. Alice pode então preparar o segundo modo de $|\Phi_B\rangle_{AB}$ aplicando a medição projetiva $\{|\psi_1\rangle\langle\psi_1|\,, |\psi_1\rangle\langle\psi_1|\}$ no primeiro modo, sendo

$$|\psi_1\rangle = \frac{1}{\sqrt{2}}(|\phi_1\rangle + |\phi_2\rangle) \tag{5.7}$$

$$|\psi_2\rangle = \frac{1}{\sqrt{2}}(|\phi_1\rangle - |\phi_2\rangle), \tag{5.8}$$

que projetará o segundo modo em um dos estados coerentes $|\gamma\rangle$ ou $|-\gamma\rangle$ com igual probabilidade. O estado $\hat{\rho}_{AB} = |\Phi_B\rangle\langle\Phi_B|_{AB}$ é certamente nG (é possível encontrar a função de Wigner em [87]) e tem vetor de médias nulo e matriz de covariância

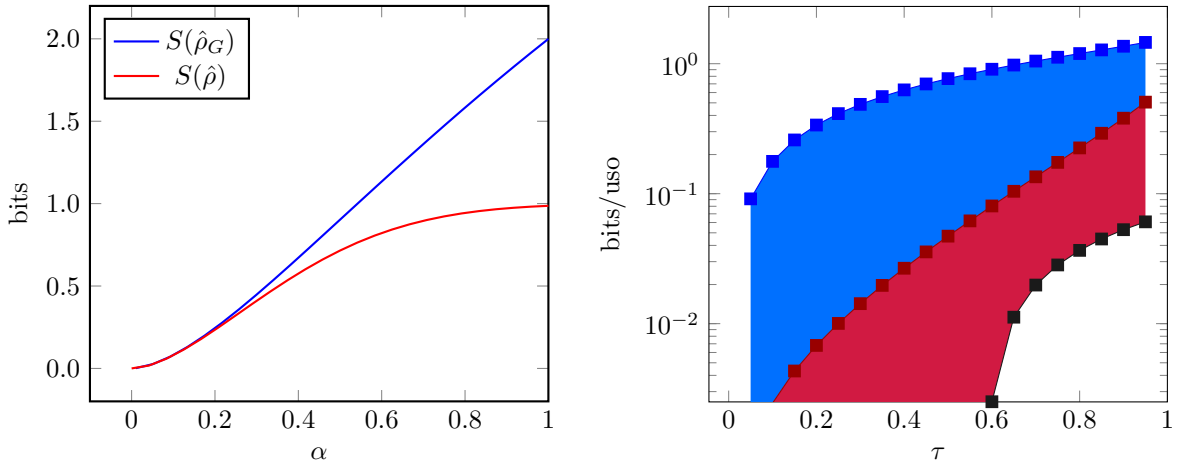
$$\boldsymbol{\Gamma}_\Phi = \begin{pmatrix} 2\alpha^2+1\boldsymbol{I} & z_2\boldsymbol{Z} \\ z_2\boldsymbol{Z} & 2\alpha^2+1\boldsymbol{I} \end{pmatrix} \xrightarrow{\mathcal{E}^{th}_{\tau,\xi}} \begin{pmatrix} 2\alpha^2+1\boldsymbol{I} & \sqrt{\tau}z_2\boldsymbol{Z} \\ \sqrt{\tau}z_2\boldsymbol{Z} & [\tau 2\alpha^2+1+\xi]\boldsymbol{I} \end{pmatrix} = \boldsymbol{\Gamma}'_\Phi \tag{5.9}$$

em que $z_2 = 2\alpha^2(1+e^{-4\alpha^2})/\sqrt{1-e^{-4\alpha^2}}$. Logo, o protocolo definido pelo estado gaussiano $\hat{\rho}^G_{AB}$ com matriz de covariância $\boldsymbol{\Gamma}_\Phi$ limita inferiormente a taxa de chave secreta do protocolo nG definido pelo estado $\hat{\rho}_{AB}$. Um terceiro parâmetro de comparação que pode ser inserido, agora um limite superior, é o protocolo de modulação gaussiana GG02, cujo estado protótipo é um TMSV (EPR) no protocolo EB equivalente descrito pela matriz na Equação (2.15) com $V = 2\alpha^2 + 1$.

Denotemos por K_{EPR}, $K(\hat{\rho})$ e $K(\rho^G_{AB})$ as taxas de chave secreta dos protocolos definidos pelo estado EPR (GG02), pela constelação BPSK P&M e pelo estado gaussiano do protocolo EB equivalente, respectivamente, as quais devem seguir a seguinte desigualdade,

$$K_{EPR} \geq K(\hat{\rho}) \geq K(\rho^G_{AB}), \tag{5.10}$$

[6] $\hat{\rho}$ define uma constelação antipodal (BPSK) rotacionada em $\pi/4$ radianos no sentido anti-horário.



(a) Entropia de uma mistura de estados coerentes e seu equivalente gaussiano.

(b) Taxas de chave secreta para o protocolo GG02, DM-CVQKD BPSK (P&M e EB).

Figura 23 – Comparativo do efeito da hipótese gaussiana (a) nas entropia de estados gaussianos e (b) na taxa de chave secreta do protocolo definido por uma mistura equiprovável de dois estados coerentes (constelação BPSK). Em (b) são traçadas as curvas de SKR para o protocolo GG02 (superior), o protcolo DM-CVQKD BPSK P&M (meio) e seu EB equivalente gaussiano (inferior), todos com mesma energia de modulação.

para energia média do esquema de modulação fixada. Na Figura 23b plotamos as curvas para as três quantidades da Equação (5.10) considerando o canal sem ruídos, $\alpha = 1$ e máxima eficiência quântica de detecção e do protocolo de reconciliação. Primeiramente, é possível ver que as desigualdades na Equação (5.10) são estritamente atendidas. A área com preenchimento em azul corresponde à lacuna de SKR, definido na Seção 3.2.1 e analisado para constelações unidimensionais, e é exatamente a área que a ser reduzida com o aumento da cardinalidade da constelação e pelos métodos de formatação. Já a área em vermelho abaixo, representa o quanto o desempenho do protocolo com constelação BPSK é *subestimado* quando a hipótese gaussiana é utilizada para analisar sua segurança e calcular a taxa de chave secreta, a qual relacionamos ao caráter não gaussiano, ou a quantidade de "não gaussianidade" (nG[7], do inglês: *non-Gaussianity*), da constelação, a ser discutido posteriormente. Apesar de que, para $\alpha << 1$, os termos de covariância do estado que define K_{EPR} e $K(\rho^G_{AB})$ se aproximem, o que justifica a aproximação acurada do primeiro pelo segundo [87], existem casos em que o valor ótimo da energia da constelação se encontra na região $\alpha > 1$ [47].

Apesar de que o protocolo EB gaussiano equivalente pode subestimar fortemente o desempenho de um protocolo DM-CVQKD, é esperado que com constelações maiores e formatadas geométrica e probabilisticamente as diferenças entre K_{EPR}, $K(\hat{\rho})$ e $K(\rho^G_{AB})$

[7]Durante o texto usaremos a sigla nG para representar os termos "não gaussiano" e "não gaussianidade", diferenciados pelo contexto.

sejam reduzidas. Ademais, o protocolo EB gaussiano equivalente a um protocolo DM-CVQKD tem papel fundamental uma vez que a estrutura teórica para prova de segurança incondicional (equivalência entre ataques coletivos e coerentes) é compatível com os protocolos definidos por estados gaussianos.

A seguir, será apresentada uma proposta para calcular a informação acessível da espiã sem a utilização da hipótese gaussiana através da decomposição do ataque de clonagem por emaranhamento realizado pela espiã por meio da decomposição de Bloch-Messiah.

5.2 Decomposição do Ataque de Clonagem por Emaranhamento[8]

Em um protocolo P&M com estados coerentes, Alice irá escolher amplitudes complexas $\{\alpha_1, \cdots, \alpha_K\}$, $\alpha_i = q_i + jp_i$ com probabilidades $\{p(\alpha_i)\}$ definindo a mistura $\mathcal{S} = \{|\alpha_i\rangle, p(\alpha_i)\}$, preparará o estado coerente $\hat{\rho}_i = |\alpha_i\rangle\langle\alpha_i|$, o envia pelo canal quântico $\mathcal{E}^{th}_{\tau,\varepsilon}$ para Bob que irá realizar detecção homódina ou heteródina com saída β_i, real ou complexa, respectivamente. Durante a comunicação quântica, Eva irá realizar o ataque físico de clonagem por emaranhamento conforme a Seção 2.2 e o esquema da Figura 24, substituindo o canal por um divisor de feixe controlado e simulando o canal térmico por meio de um estado TMSV.

O estado coerente $\hat{\rho}_i$ preparado por Alice e o estado auxiliar TMSV $\hat{\rho}_{CE} = |\nu\rangle\langle\nu|_{CE}$, com ruído de quadratura $\nu = 2\bar{n} + 1$, preparado por Eva são inicialmente descorrelacionados e tem os modos A e C acoplados pelo divisor de feixe, representado pelo operador $\hat{B}_{AC}(\tau)$, e o sistema tripartido ACE evolui de acordo com a operação unitária $\hat{B}_T = \hat{B}_{AC}(\tau) \otimes \hat{I}_E$. Os modos de saída B e D do divisor de feixe (e o modo E que não foi acoplado) irão evoluir para o estado descrito por

$$\hat{\rho}_{BDE} = \hat{B}_T(\hat{\rho}_i \otimes \hat{\rho}_{CE})\hat{B}_T^\dagger, \tag{5.11}$$

de modo que os estados de Bob em função do ruído térmico induzido pelo TMSV e o estado de Eva após a operação, dado que Alice enviou o i-ésimo estado do conjunto, serão

$$\hat{\rho}_{Bob|i} = \mathrm{tr}_{DE}(\hat{B}_T(\hat{\rho}_i \otimes \hat{\rho}_{CE})\hat{B}_T^\dagger), \qquad \hat{\rho}_{Eva|i} = \mathrm{tr}_B(\hat{B}_T(\hat{\rho}_i \otimes \hat{\rho}_{CE})\hat{B}_T^\dagger). \tag{5.12}$$

Entretanto, calcular os traços parciais nas equações em 5.12 não é tarefa simples uma vez que o divisor de feixe imprime correlações entre os três modos. De fato, é possível

[8] Os resultados desta seção foram publicados no *International Workshop on Quantum Communication and Quantum Cryptography* - IEEE CNS 2021, [88].

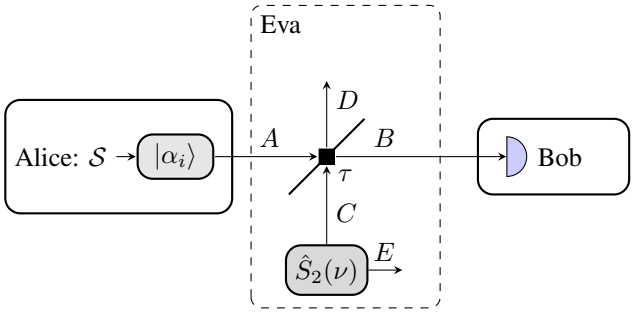


Figura 24 – Modelo do canal quântico com ruído térmico resultante do ataque de clonagem por emaranhamento.

explicitar o estado tripartido na saída da operação pela evolução dos operadores de modo $\hat{a}$, $\hat{c}$ e $\hat{e}$ pela transformação de Bogoliubov induzida pelo divisor de feixe (Exemplo A.12)

$$\hat{a} \xrightarrow{\hat{B}_T} \hat{b} = t\hat{a} + r\hat{c}, \tag{5.13}$$

$$\hat{c} \xrightarrow{\hat{B}_T} \hat{d} = -r\hat{a} + t\hat{c}, \tag{5.14}$$

de modo que, escrevendo os estados iniciais como a atuação dos operadores de deslocamento e compressão de dois modos no estado tripartido de vácuo nos modos ACE, temos que

$$|\alpha_i\rangle_A |\nu\rangle_{CE} = \hat{D}_A(\alpha_i) \otimes \hat{S}_2(z) |000\rangle_{ACE}\,, \tag{5.15}$$

$$= \exp\{\alpha\hat{a}^\dagger - \alpha^*\hat{a}\} \otimes \exp\left\{\frac{z}{2}(\hat{c}\hat{e} - \hat{c}^\dagger\hat{e}^\dagger)\right\} |000\rangle_{ACE}\,, \tag{5.16}$$

e aplicando as substituições $\hat{a} = t\hat{b} - r\hat{d}$ e $\hat{c} = r\hat{b} + t\hat{d}$ induzidas pelo divisor de feixe, temos que

$$\exp\{\alpha\hat{a}^\dagger - \alpha^*\hat{a}\} \to \exp\left\{\alpha(t\hat{b}^\dagger - r\hat{d}^\dagger) - \alpha^*(t\hat{b} - r\hat{d})\right\} = \hat{D}_B(t\alpha) \otimes \hat{D}_D(-r\alpha), \tag{5.17}$$

$$\exp\left\{\frac{z}{2}(\hat{c}\hat{e} - \hat{c}^\dagger\hat{e}^\dagger)\right\} \to \exp\left\{\frac{z}{2}((r\hat{b} + t\hat{d})\hat{e} - (r\hat{b}^\dagger + t\hat{d}^\dagger)\hat{e}^\dagger)\right\}, \tag{5.18}$$

resultando no seguinte estado na saída do divisor de feixe,

$$|\alpha_i\rangle_A |\nu\rangle_{CE} \xrightarrow{\hat{B}_T} \hat{D}_B(t\alpha_i)\hat{D}_D(-r\alpha_i) \exp\left\{\frac{zt}{2}(\hat{e}\hat{d} - \hat{e}^\dagger\hat{d}^\dagger) + \frac{zr}{2}(\hat{e}\hat{b} - \hat{e}^\dagger\hat{b}^\dagger)\right\} |000\rangle_{BDE}\,, \tag{5.19}$$

sendo $t = \sqrt{\tau}$, $r = \sqrt{1-\tau}$ e $z = \frac{1}{2}\cosh^{-1}(\nu)$. Os operadores de deslocamento que surgem na Equação (5.19) são independentes (no sentido de separabilidade) mas a evolução do operador de compressão de dois modos indica o emaranhamento entre os três modos BDE e não é separável.

Outra forma de analisar a evolução dos estados é por meio das respectivas representações no espaço de fase uma vez que os estados e operações em envolvidos em

uma rodada do protocolo são todos gaussianos[9]. Podemos representar o ataque de clonagem por emaranhamento para o protocolo P&M utilizando a transformação simplética do BS nas matrizes de covariância e vetor de deslocamento. O estado inicial dos sistemas composto de Alice e Eva será descrito por

$$\langle \hat{\boldsymbol{r}}_i \rangle = (q_i, p_i, 0, 0, 0, 0)^T \tag{5.20}$$

$$\boldsymbol{\Sigma}_i = \begin{pmatrix} \boldsymbol{I} & 0 & 0 \\ 0 & (2\bar{n}+1)\boldsymbol{I} & 2\sqrt{\bar{n}^2+\bar{n}}\boldsymbol{I} \\ 0 & 2\sqrt{\bar{n}^2+\bar{n}}\boldsymbol{I} & (2\bar{n}+1)\boldsymbol{I} \end{pmatrix}, \tag{5.21}$$

e a operação realizada pelo divisor de feixe acopla os modos A e C conforme a matriz simplética expandida

$$\boldsymbol{B}_T = \begin{pmatrix} t\boldsymbol{I} & r\boldsymbol{I} & 0 \\ -r\boldsymbol{I} & t\boldsymbol{I} & 0 \\ 0 & 0 & \boldsymbol{I} \end{pmatrix}. \tag{5.22}$$

A operação de clonagem por emaranhamento faz a matriz de covariância e vetor de médias evoluírem da seguinte maneira

$$\boldsymbol{B}_T \langle \hat{\boldsymbol{r}}_i \rangle = (tq_i, tp_i, -rq_i, -rp_i, 0, 0)^T, \tag{5.23}$$

$$\boldsymbol{B}_T \boldsymbol{\Sigma} \boldsymbol{B}_T^T = \begin{pmatrix} (2r^2\bar{n}+1)\boldsymbol{I} & 2tr\bar{n}\boldsymbol{I}_2 & 2r\sqrt{\bar{n}^2+\bar{n}}\boldsymbol{Z} \\ 2tr\bar{n}\boldsymbol{I} & (2t^2\bar{n}+1)\boldsymbol{I} & 2t\sqrt{\bar{n}^2+\bar{n}}\boldsymbol{Z} \\ 2r\sqrt{\bar{n}^2+\bar{n}}\boldsymbol{Z} & 2t\sqrt{\bar{n}^2+\bar{n}}\boldsymbol{Z} & (2\bar{n}+1)\boldsymbol{I} \end{pmatrix}, \tag{5.24}$$

que é a representação do estado dos modos B, D e E para um uso do canal. Logo, o estado recebido por Bob é descrito pelo vetor de deslocamento $\langle \hat{\boldsymbol{r}}_{Bob|i} \rangle = (\sqrt{\tau}q_i, \sqrt{\tau}p_i)^T$ e pela matriz $\boldsymbol{\Sigma}_{Bob} = (2(1-\tau)\bar{n}+1)\boldsymbol{I}$, ou seja, um estado térmico com número médio de fótons $(1-\tau)\bar{n}$ e deslocado em $\sqrt{\tau}\alpha$, $\hat{\rho}^{th}(\sqrt{\tau}\alpha_i, (1-\tau)\bar{n})$. Para Eva, descartando o sistema de Bob, temos que

$$\langle \hat{\boldsymbol{r}} \rangle_{Eva|i} = (-rq_i, -rp_i, 0, 0)^T \tag{5.25}$$

$$\boldsymbol{\Sigma}_{Eva} = \begin{pmatrix} (2t^2\bar{n}+1)\boldsymbol{I} & 2t\sqrt{\bar{n}^2+\bar{n}}\boldsymbol{Z} \\ 2t\sqrt{\bar{n}^2+\bar{n}}\boldsymbol{Z} & (2\bar{n}+1)\boldsymbol{I} \end{pmatrix} = \begin{pmatrix} a\boldsymbol{I} & c\boldsymbol{Z} \\ c\boldsymbol{Z} & b\boldsymbol{I} \end{pmatrix}. \tag{5.26}$$

Para cada uso do canal, Bob espera a mistura $\hat{\rho}_B = \sum_i p(\alpha_i)\hat{\rho}^{th}(\sqrt{\tau}\alpha_i, (1-\tau)\bar{n})$ e cada estado térmico deslocado recebido no laboratório apresentará a seguinte função de distribuição de probabilidades na detecção das quadraturas

$$p(\beta|\alpha_i)(\bar{n}) = \begin{cases} \sqrt{\frac{2}{\pi(2\bar{n}+1)}} e^{-2(\beta-\sqrt{\tau}\alpha_{i,\theta})^2/(2\bar{n}+1)}, \text{ detecção homódina}[10], \\ \frac{1}{\pi(1+(1-\tau)\bar{n})} e^{|\beta-\sqrt{\tau}\alpha_i|^2/(1+(1-\tau)\bar{n})}, \text{ detecção heteródina}, \end{cases} \tag{5.27}$$

[9]Destacamos que em uma única rodada, isto é, um uso do canal, não há não gaussianidade. O fator não gaussiano surge quando observamos o conjunto de estados que Alice prepara.

de modo que a informação mútua $I(A;B)$ pode ser calculada analogamente ao caso do canal sem ruídos abordado nas Seções 3.2.1 e 3.2.2.

O cálculo da informação acessível a Eva envolve algumas sutilezas adicionais. Ocorre que o limitante de Holevo depende das entropias de von Neumann $S(\hat{\rho}_{Eva})$ e $S(\hat{\rho}_{Eva|b})$, sendo

$$\hat{\rho}_{Eva} = \sum_i p_i \hat{\rho}_{Eva|i}, \qquad \hat{\rho}_{Eva|b} = \sum_i p(\alpha_i|\beta)\hat{\rho}_{Eva|i}, \tag{5.28}$$

de modo que se faz necessária uma descrição dos estados após a interação. Podemos então discutir a evolução do sistema bipartido de Eva como iniciando em um estado TMSV $|\nu\rangle_{CE}$ e sendo submetido a uma operação $\hat{U}_i$ ainda desconhecida e que está condicionada ao estado coerente $\hat{\rho}_i$ enviado por Alice. Então, como para cada estado de Alice Eva prepara um TMSV, a mistura preparada por Alice induz uma *mistura não gaussiana de estados* $\hat{\rho}_{Eva} = \sum_i p_i \hat{U}_i |\nu\rangle\langle\nu| \hat{U}_i^\dagger$ nos modos do sistema de Eva de modo que

$$\chi(E,B) = S(\hat{\rho}_{Eva}) - \int p(b) S(\hat{\rho}_{Eva|b})\, \mathrm{d}b\,, \tag{5.29}$$

$$= S\left(\sum_i p_i \hat{U}_i |\nu\rangle\langle\nu| \hat{U}_i^\dagger\right) - \int p(b) \left(\sum_i p(\alpha_i|b)\hat{U}_i |\nu\rangle\langle\nu| \hat{U}_i^\dagger\right). \tag{5.30}$$

Uma vez que $\hat{\rho}_{Eva|i}$ é um estado gaussiano[11] a decomposição térmica da matriz de covariância da Equação (5.26) indica que existe uma operação unitária canônica $\hat{U}_C$ que, aplicada a um estado térmico de dois modos

$$\hat{\sigma}^{\oplus} = \bigotimes_{k=1}^{2} \hat{\rho}^{th}\left(\frac{\nu_k - 1}{2}\right), \tag{5.31}$$

em que ν_k são os autovalores simpléticos de $\boldsymbol{\Sigma}_{Eva}$ (Equação (5.26)), em conjunto com uma operação de deslocamento $\hat{D}(\boldsymbol{\beta}_i) = \hat{D}_D(-\sqrt{1-\tau}\alpha_i) \otimes \hat{I}_E$, $\boldsymbol{\beta}_i = (-\sqrt{1-\tau}\alpha_i, 0)^T$, é possível obter a identidade $\hat{\rho}_{Eva|i} = \hat{D}(\boldsymbol{\beta}_i)\hat{U}_C\hat{(}\sigma^{\oplus})\hat{U}_C^\dagger\hat{D}(\boldsymbol{\beta}_i)^\dagger$. Embora o operador $\hat{U}_C$ ainda seja desconhecido, a decomposição de Bloch-Messiah [89] (também conhecida como decomposição de Euler) afirma que é possível decompor operações unitárias arbitrárias como a combinação de rotações de vários modos e um conjunto paralelo de compressões de um modo arranjadas de maneira adequada. De fato, veremos que, para as quantidades entrópicas, é possível substituir o conjunto não gaussiano de estados de Eva como sendo equivalente a um conjunto de estados térmicos deslocados. Nas próximas seções, a decomposição será apresentada e aplicada ao esquema de ataque de

[10] Nesse caso, θ indica a fase relativa entre o sinal e o oscilador local da detecção homódina. Logo, $\alpha_{i,0} = \mathrm{Re}\{\alpha\}$ e $\alpha_{i,\pi/2} = \mathrm{Im}\{\alpha\}$.

[11] Todas as operações que resultam em $\hat{\rho}_{Eva|i}$ são gaussianas: divisor de feixe e traço parcial.

clonagem por emaranhamento. Adicionalmente, será apresentado um exemplo de como a decomposição de Bloch-Messiah proporciona limitantes mais acurados para a informação de Holevo da espiã.

5.2.1 A Decomposição de Bloch-Messiah

A decomposição de Bloch-Messiah (BMD, do inglês: *Bloch-Messiah Decomposition*) usa uma solução específica simultânea e "condicionada" da Decomposição em Valores Singulares (SVD, do inglês: *Singular Value Decomposition*) das matrizes de Bogoliubov $\boldsymbol{E}$ e $\boldsymbol{F}$ que definem uma operação unitária para obter uma combinação de rotações, compressões e deslocamentos equivalente à operação original [89, 90, 91].

Teorema 5.2 (Decomposição de Bloch-Messiah [89])**.** *Sejam $\boldsymbol{E}$ e $\boldsymbol{F}$ matrizes de Bogoliubov correspondendo a uma transformação unitária arbitrária. É possível encontrar uma decomposição específica da forma*

$$\boldsymbol{E} = \boldsymbol{U}\boldsymbol{\Lambda}_{\boldsymbol{E}}\boldsymbol{W}_E^{\dagger}, \qquad \boldsymbol{F} = \boldsymbol{U}\boldsymbol{\Lambda}_{\boldsymbol{F}}\boldsymbol{W}_F^{\dagger}, \tag{5.32}$$

em que $\boldsymbol{U}$, $\boldsymbol{W}_E$ e $\boldsymbol{W}_F$ são matrizes unitárias que satisfazem a condição

$$\boldsymbol{W}_F = \boldsymbol{W}_E^{*}, \tag{5.33}$$

que é chamada de condição de rotação e $\boldsymbol{\Lambda}_E$ e $\boldsymbol{\Lambda}_F$ são diagonais com elementos não-negativos satisfazendo

$$\boldsymbol{\Lambda}_E = \boldsymbol{I} + \boldsymbol{\Lambda}_F. \tag{5.34}$$

Como afirmado anteriormente, a decomposição de Bloch-Messiah requer uma SVD específica em ambas as matrizes de Bogoliubov que representam a operação Gaussiana arbitrária. Uma das especificidades é que a solução deve ter a mesma matriz unitária à esquerda, o que é possível uma vez que $\boldsymbol{E}$ e $\boldsymbol{F}$ são diagonais na mesma base. Em segundo lugar, e mais sutil, a Equação (5.33) estabelece que as matrizes unitárias à direita da decomposição não são arbitrárias. Essa condição nem sempre é satisfeita para uma solução arbitrária da SDV e o seguinte procedimento deve ser realizado: (i) realizar o SVD que satisfaça Equação (5.32), a qual possivelmente não satisfará a condição de rotação, e (ii) das matrizes $\boldsymbol{W}_E$ e $\boldsymbol{W}_F$ obtidas, calcular a matriz de balanceamento $\boldsymbol{D}$ pela fatoração de Takagi conforme definido abaixo [90].

Teorema 5.3 (Fatoração de Takagi [92, Corolário 4.4.4])**.** *Uma matriz $N \times N$ complexa e simétrica $\boldsymbol{A}$ pode ser decomposta da seguinte forma,*

$$\boldsymbol{A} = \boldsymbol{U}_A\boldsymbol{\Lambda}_A\boldsymbol{U}_A^{T}, \tag{5.35}$$

em que $\boldsymbol{U}_A$ é uma matriz unitária e $\boldsymbol{\Lambda}_A$ é diagonal com entradas não negativas, os valores singulares de $\boldsymbol{A}$. Particularmente, se $\boldsymbol{A}$ é simétrica e unitária,

$$\boldsymbol{A} = \boldsymbol{U}_A \boldsymbol{U}_A^T \longrightarrow \boldsymbol{U}_A = \boldsymbol{A}^{1/2}. \tag{5.36}$$

Então, a partir das matrizes $\boldsymbol{W}_E$ e $\boldsymbol{W}_F$ calculamos a matriz $\boldsymbol{G} = \boldsymbol{W}_E^\dagger \boldsymbol{W}_F^*$ que é diagonal em blocos, unitária e simétrica e, de acordo com a fatoração de Takagi, $\boldsymbol{G} = \boldsymbol{D}\boldsymbol{D}^T$. Então, podemos concluir a BMD introduzindo a matriz de balanceamento $\boldsymbol{D}$ nas matrizes unitárias anteriores como $\boldsymbol{\mathcal{U}} = \boldsymbol{U}\boldsymbol{D}$, $\boldsymbol{\mathcal{W}}_E = \boldsymbol{W}_F^* \boldsymbol{D}^*$ e $\boldsymbol{\mathcal{W}}_F = \boldsymbol{W}_F \boldsymbol{D}$, que resulta em

$$\boldsymbol{E} = \boldsymbol{\mathcal{U}} \boldsymbol{\lambda}_E \boldsymbol{\mathcal{W}}_E^\dagger, \qquad\qquad \boldsymbol{F} = \boldsymbol{\mathcal{U}} \boldsymbol{\lambda}_F \boldsymbol{\mathcal{W}}_F^\dagger \tag{5.37}$$

5.2.2 Decomposição do Ataque de Clonagem por Emaranhamento

Como apresentado, a BMD é utilizada para decompor as matrizes de Bogoliubov que descrevem a evolução do sistema quântico. Logo, é necessário derivar as respectivas matrizes que correspondem à evolução do sistema da espiã dado que o estado inicial é um estado TMSV, e então obter uma nova perspectiva sobre o ataque de clonagem por emaranhamento. Partindo da matriz de covariância de Eq. (5.26), observamos sua forma padrão [64] para a qual os autovalores simpléticos são dados por

$$\nu_{1,2} = \frac{\sqrt{(a+b)^2 - 4c^2} \pm (b-a)}{2} \tag{5.38}$$

e a matriz simplética para a decomposição térmica $\boldsymbol{\Sigma}_{\boldsymbol{Eva}} = \boldsymbol{S}\boldsymbol{\Sigma}_{\boldsymbol{Eva}}^{\oplus}\boldsymbol{S}^T$ é dada por

$$\boldsymbol{S} = \begin{pmatrix} w_1 \boldsymbol{I} & w_2 \boldsymbol{Z} \\ w_2 \boldsymbol{Z} & w_1 \boldsymbol{I}, \end{pmatrix}, \qquad\qquad w_{1,2} = \sqrt{\frac{a+b}{2\sqrt{(a+b)^2 - 4c^2}} \pm \frac{1}{2}}. \tag{5.39}$$

Partindo de $\boldsymbol{S}$, podemos calcular as matrizes de Bogoliubov usando as relações entre os operadores bosônicos e de quadratura. Logo,

$$\hat{\boldsymbol{r}}^b = \boldsymbol{S}\hat{\boldsymbol{r}}^a \Rightarrow \begin{pmatrix} \hat{q}_1^b \\ \hat{p}_1^b \\ \hat{q}_2^b \\ \hat{p}_2^b \end{pmatrix} = \begin{pmatrix} w_1 & 0 & w_2 & 0 \\ 0 & w_1 & 0 & -w_2 \\ w_2 & 0 & w_1 & 0 \\ 0 & -w_2 & 0 & w_1 \end{pmatrix} \begin{pmatrix} \hat{q}_1^a \\ \hat{p}_1^a \\ \hat{q}_2^a \\ \hat{p}_2^a \end{pmatrix} \tag{5.40}$$

em que $\hat{\boldsymbol{a}}$ e $\hat{\boldsymbol{b}}$ são os vetores de operadores bosônicos, $\hat{\boldsymbol{r}}$ o vetor de operadores de quadratura onde usamos o sobrescrito para indicar os modos de entrada e saída da operação (a e b, respectivamente). Logo, fazendo as substituições $\hat{q}_i = \hat{a}_i + \hat{a}_i^\dagger$ e $\hat{p}_i = -j(\hat{a}_i - \hat{a}_i^\dagger)$ e realizando

operações elementares de linhas para isolar os operadores bosônicos, temos que

$$\begin{pmatrix} \hat{b}_1 \\ \hat{b}_2 \\ \hat{b}_1^\dagger \\ \hat{b}_2^\dagger \end{pmatrix} = \begin{pmatrix} w_1 & 0 & w_2 & 0 \\ 0 & w_1 & 0 & -w_2 \\ w_2 & 0 & w_1 & 0 \\ 0 & -w_2 & 0 & w_1 \end{pmatrix} \begin{pmatrix} \hat{a}_1 \\ \hat{a}_2 \\ \hat{a}_1^\dagger \\ \hat{a}_2^\dagger \end{pmatrix}. \tag{5.41}$$

Logo,

$$\begin{pmatrix} \hat{\boldsymbol{b}} \\ \hat{\boldsymbol{b}}^\dagger \end{pmatrix} = \begin{pmatrix} w_1\boldsymbol{I} & w_2\boldsymbol{X} \\ w_2\boldsymbol{X} & w_1\boldsymbol{I} \end{pmatrix} \begin{pmatrix} \hat{\boldsymbol{a}} \\ \hat{\boldsymbol{a}}^\dagger \end{pmatrix} \tag{5.42}$$

Então, $\boldsymbol{E} = w_1\boldsymbol{I}$ e $\boldsymbol{F} = w_2\boldsymbol{X}$ são as matrizes de Bogoliubov correspondentes à matriz simplética $\boldsymbol{S}$. A partir das matrizes Bogoliubov obtidas em Equação (5.42), aplicamos a decomposição descrita na seção anterior para obter a estrutura da BMD de Eva:

1. Valores singulares de $\boldsymbol{E}$ e $\boldsymbol{F}$:

$$\boldsymbol{E}\boldsymbol{E}^\dagger = w_1^2\boldsymbol{I}, \qquad \boldsymbol{F}\boldsymbol{F}^\dagger = w_2^2\boldsymbol{I}, \tag{5.43}$$

   uma vez que $w_1, w_2 \in \mathbb{R}$.

2. Decomposição por Valores Singulares de $\boldsymbol{E}$ e $\boldsymbol{F}$:

$$\boldsymbol{E} = \boldsymbol{I}\boldsymbol{\Lambda}_E\boldsymbol{I} = \boldsymbol{U}\boldsymbol{\Lambda}_E\boldsymbol{W}_E^\dagger, \tag{5.44}$$

$$\boldsymbol{F} = \boldsymbol{I}\boldsymbol{\Lambda}_F\boldsymbol{X} = \boldsymbol{U}\boldsymbol{\Lambda}_F\boldsymbol{W}_F^\dagger, \tag{5.45}$$

   em que a SDV da matriz $\boldsymbol{E}$ é o caso trivial e sendo $\boldsymbol{\Lambda}_E = \mathrm{diag}(w_1, w_1)$ e $\boldsymbol{\Lambda}_F = \mathrm{diag}(w_2, w_2)$ as matrizes diagonais que correspondem às operações de compressão, $\boldsymbol{W}_E^\dagger = \boldsymbol{I}$ e $\boldsymbol{W}_F^\dagger = \boldsymbol{X}$ são as matrizes de rotação à direita, as quais não satisfazem às condições de rotação.

3. Calcular $\boldsymbol{G} = \boldsymbol{W}_E^\dagger\bar{\boldsymbol{W}}_F$:

$$\boldsymbol{W}_E^\dagger\bar{\boldsymbol{W}}_F = \boldsymbol{X}. \tag{5.46}$$

4. Calcular a matriz de balanceamento usando o Teorema 5.3 (Fatoração de Takagi),

$$\boldsymbol{G} = \boldsymbol{D}\boldsymbol{D}^T \rightarrow \boldsymbol{D} = \boldsymbol{G}^{\frac{1}{2}} = \boldsymbol{X}^{\frac{1}{2}} \tag{5.47}$$

$$\boldsymbol{D} = \frac{1}{\sqrt{2}} \begin{pmatrix} e^{i\pi/4} & e^{-i\pi/4} \\ e^{-i\pi/4} & e^{i\pi/4}. \end{pmatrix} \tag{5.48}$$

5. Calcular as matrizes de rotação à esquerda e à direita usando a matriz de balanceamento $\boldsymbol{D}$,

$$\boldsymbol{\mathcal{W}}_E^\dagger = \boldsymbol{D}^T\boldsymbol{W}_F^T = \frac{1}{\sqrt{2}} \begin{pmatrix} e^{-i\pi/4} & e^{\pi/4} \\ e^{i\pi/4} & e^{-i\pi/4} \end{pmatrix}, \tag{5.49}$$

$$\boldsymbol{\mathcal{U}} = \boldsymbol{U}\boldsymbol{D} = \frac{1}{\sqrt{2}} \begin{pmatrix} e^{i\pi/4} & e^{-i\pi/4} \\ e^{-i\pi/4} & e^{i\pi/4} \end{pmatrix}. \tag{5.50}$$

e $\boldsymbol{\mathcal{W}}_F = \boldsymbol{\mathcal{W}}_E^*$.

Com as matrizes apropriadas, concluímos que a BMD da transformação unitária canônica $\hat{U}_C$ a qual o estado da espiã está submetida, representada pelas matrizes de Bogoliubov $\boldsymbol{E} = \boldsymbol{\mathcal{U}}\boldsymbol{\Lambda}_E\boldsymbol{\mathcal{W}}_E^\dagger$ e $\boldsymbol{F} = \boldsymbol{\mathcal{U}}\boldsymbol{\Lambda}_F\boldsymbol{\mathcal{W}}_F^\dagger$, corresponde a uma operação de rotação $\hat{R}_{\boldsymbol{\phi}_1}$, com $e^{i\boldsymbol{\phi}_1} = \boldsymbol{\mathcal{W}}_E^\dagger$, um conjunto de compressões de um modo em paralelo $\hat{S}_{\boldsymbol{r}}$ em que $\cosh(\boldsymbol{r}) = \boldsymbol{\Lambda}_E$ e $\sinh(\boldsymbol{r})e^{i\boldsymbol{\theta}} = \boldsymbol{\Lambda}_F$, e uma segunda operação de rotação com operador $\hat{R}_{\boldsymbol{\phi}_2}$ com $e^{i\boldsymbol{\phi}_2} = \boldsymbol{\mathcal{U}}$, ou seja,

$$\hat{U}_C = \hat{R}_{\boldsymbol{\phi}_2}\hat{S}_{\boldsymbol{r}}\hat{R}_{\boldsymbol{\phi}_1}. \tag{5.51}$$

Então, ao incluir o deslocamento, o estado TMSV pode ser visto como passando pela seguinte transformação:

$$|\nu\rangle\langle\nu|_{CE} \longrightarrow \hat{D}_{\boldsymbol{\beta}_i}\hat{R}_{\boldsymbol{\phi}_2}\hat{S}_{\boldsymbol{r}}\hat{R}_{\boldsymbol{\phi}_1}\left[\hat{\rho}_{\nu_1'}^{th} \otimes \hat{\rho}_{\nu_2'}^{th}\right]\hat{R}_{\boldsymbol{\phi}_1}^\dagger\hat{S}_{\boldsymbol{r}}^\dagger\hat{R}_{\boldsymbol{\phi}_2}^\dagger\hat{D}_{\boldsymbol{\beta}_i}^\dagger = \hat{\rho}_{Eva|i}, \tag{5.52}$$

com $\hat{\rho}_{\nu_i'}^{th}$ o estado térmico com número médio de fótons ν_i', $\nu_1' = (\nu_1 - 1)/2$ e $\nu_2' = (\nu_2 - 1)/2$. É possível inverter a ordem dos operadores aplicando as regras de comutação entre $\hat{D}$, $\hat{R}$ e $\hat{S}$ de modo que

$$\hat{D}_{\boldsymbol{\beta}_i}\hat{R}_{\boldsymbol{\phi}_2}\hat{S}_{\boldsymbol{r}}\hat{R}_{\boldsymbol{\phi}_1} = \hat{R}_{\boldsymbol{\phi}_2}\hat{S}_{\boldsymbol{r}}\hat{R}_{\boldsymbol{\phi}_1}\hat{D}_{\boldsymbol{\beta}_i'}, \tag{5.53}$$

em que o vetor de deslocamento $\boldsymbol{\beta}_i$ será

$$\begin{aligned} \boldsymbol{\beta}_i' &= e^{-i\boldsymbol{\phi}_1}\cosh(\boldsymbol{r})e^{-i\boldsymbol{\phi}_2}\boldsymbol{\beta}_i - e^{-i\boldsymbol{\phi}_1}\sinh(\boldsymbol{r})e^{i\boldsymbol{\phi}_2}\boldsymbol{\beta}_i^* && (5.54)\\ &= \boldsymbol{\mathcal{W}}_E^T\boldsymbol{\Lambda}_E\boldsymbol{\mathcal{U}}^*\boldsymbol{\beta}_i - \boldsymbol{\mathcal{W}}_E^T\boldsymbol{\Lambda}_F\boldsymbol{\mathcal{U}}\boldsymbol{\beta}_i^* && (5.55)\\ &= w_1\boldsymbol{\beta}_i - w_2\boldsymbol{\sigma}_X\boldsymbol{\beta}_i^* && (5.56)\\ &= (-w_1 r\alpha_i, w_2 r\alpha_i^*)^T, && (5.57) \end{aligned}$$

com vetor $(-w_1 rq_i, -w_1 rp_i, w_2 rq_i, -w_2 rp_i)^T$ correspondente no espaço de fase. Então, o estado da espiã após a operação de clonagem por emaranhamento corresponde a

$$\hat{\rho}_{Eve|i} = \hat{U}_C\hat{D}_{\boldsymbol{\beta}_i'}\left[\hat{\rho}_{\nu_1'}^{th} \otimes \hat{\rho}_{\nu_2'}^{th}\right]\hat{D}_{\boldsymbol{\beta}_i'}^\dagger\hat{U}_C^\dagger, \tag{5.58}$$

Logo, a operação canônica $\hat{U}_C$ atua em um estado térmico bipartido deslocado e separável. Uma vez que as amplitudes dos estados preparados por Alice têm influência apenas sobre os deslocamentos $\boldsymbol{\beta}_i$ e a entropia de von Neumann é invariante sob operações unitárias, temos que

$$S(\hat{\rho}_{Eva}) = S\left(\sum_i p(\alpha_i)\hat{\rho}_{Eva|i}\right) = S\left(\sum_i p(\alpha_i)\hat{D}_{\boldsymbol{\beta}_i'}\hat{\rho}_{\nu_1'}^{th} \otimes \hat{\rho}_{\nu_2'}^{th}\hat{D}_{\boldsymbol{\beta}_i'}^\dagger\right), \tag{5.59}$$

$$S(\hat{\rho}_{Eva|b}) = S\left(\sum_i p(\alpha_i|b)\hat{\rho}_{Eva|i}\right) = S\left(\sum_i p(\alpha_i|b)\hat{D}_{\boldsymbol{\beta}'_i}\hat{\rho}^{th}_{\nu'_1} \otimes \hat{\rho}^{th}_{\nu'_2}\hat{D}^{\dagger}_{\boldsymbol{\beta}'_i}\right), \tag{5.60}$$

ou seja, as quantidades entrópicas envolvendo o estado da espiã são iguais às de um conjunto de estados térmicos bipartidos deslocados denotados por $\hat{\upsilon}$,

$$\hat{\upsilon} = \sum_i p(\alpha_i)\hat{D}_{\boldsymbol{\beta}'_i}\hat{\rho}^{th}_{\nu'_1} \otimes \hat{\rho}^{th}_{\nu'_2}\hat{D}^{\dagger}_{\boldsymbol{\beta}'_i} \tag{5.61}$$

Mesmo tendo simplificado as expressões para calcular a quantidade de Holevo na Equação (5.30) removendo a operação unitária canônica $\hat{U}_C$, ou seja, "desemaranhando" o estado emaranhado da espiã, calcular a entropia de um conjunto de estados térmicos deslocados não é trivial devido ao seu caráter não gaussiano.Logo, será lançado mão mais uma vez da hipótese gaussiana para calcular um limitante superior para $S(\hat{\rho}_{Eva})$ utilizando o estado gaussiano equivalente $\hat{\upsilon}^G$. Contudo, será visto nos resultados apresentados que o limitante calculado com o estado decomposto reduz a superestimação das quantidades de informação da espiã.

5.2.3 Aplicação: a Constelação Quaternária

Vamos tomar como exemplo um protocolo DM-CVQKD baseado em constelação QPSK [8] e aplicar a BMD desenvolvida para calcular a entropia do conjunto de estados induzido no sistema da espiã durante o ataque de clonagem por emaranhamento. A implementação do protocolo DM-CVQKD do tipo P&M com constelação QPSK consiste em Alice preparar estados coerentes $\{|\alpha_1\rangle, |\alpha_2\rangle, |\alpha_3\rangle, |\alpha_4\rangle\}$ equiprováveis com $\alpha_i = \alpha e^{j\theta_i}$, $\theta_i = (2i-1)\pi/4$, enviá-los através de um canal quântico linear gaussiano com transmitância τ e ruído térmico $\bar{n}$ e Bob realizará a detecção de heteródino na recepção. De acordo com a Equação (5.25), cada i-ésimo estado coerente preparado por Alice, quando interceptado pela máquina de clonagem de Eva, resulta no deslocamento $\boldsymbol{\beta}_i = (-r\alpha e^{j\theta_i}, 0)^T$ nos modos D e E (Figura 24) e é transformado para $\boldsymbol{\beta}'_i = (-w_1 r\alpha e^{j\theta_i}, w_2 r\alpha e^{-j\theta_i})^T$, Equação (5.57), de modo que a mistura $\hat{\upsilon}_Q$ de estados térmicos induzida pela constelação QPSK será,

$$\hat{\upsilon}_Q = \frac{1}{4}\sum_{i=0}^{3} \hat{D}_{\boldsymbol{\beta}'_i}\hat{\rho}^{th}_{\nu'_1} \otimes \hat{\rho}^{th}_{\nu'_2}\hat{D}^{\dagger}_{\boldsymbol{\beta}'_i} = \frac{1}{4}\sum_{i=0}^{3} \hat{\upsilon}_i, \tag{5.62}$$

em que $\nu'_i = (\nu_i - 1)/2$ é obtido dos autovalores simpléticos da matriz na Equação (5.26) e $w_{1,2}$ calculados pela Equação (5.39) e a entropia da mistura observada por Eva é exatamente $S(\hat{\upsilon}_Q)$.

Foi visto na seção anterior que é possível limitar superiormente $S(\hat{\upsilon}_Q)$ utilizando a hipótese gaussiana (GET), tratando o estado $\hat{\upsilon}_Q$ como se fosse descrito pelos dois primeiros

momentos estatísticos. Isso implica que $S(\hat{\rho}_{Eva}) = S(\hat{v}_Q) \leq S(\hat{v}_Q^G) = g(\iota_1) + g(\iota_2)$, sendo $\{\iota_i\}$ os autovalores simpléticos da matriz de covariância $\mathbf{\Gamma}(\hat{v}_Q)$ e $g(\cdot)$ a função entrópica bosônica, definida na Equação (B.17). Usando as identidades envolvendo o operador de deslocamento de um modo e os operadores bosônicos,

$$\begin{aligned} \hat{D}_d\hat{D}_d^\dagger &= \hat{I}, & \hat{D}_d^\dagger\hat{a}^2\hat{D}_x &= (\hat{a}+d)(\hat{a}+d), \\ \hat{D}_d^\dagger\hat{a}\hat{D}_d &= \hat{a}+d, & \hat{D}_d^\dagger\hat{a}^{\dagger 2}\hat{D}_x &= (\hat{a}^\dagger+d^*)(\hat{a}^\dagger+d^*), \\ \hat{D}_d^\dagger\hat{a}^\dagger\hat{D}_d &= \hat{a}^\dagger+d^*, & \hat{D}_d^\dagger\hat{a}\hat{a}^\dagger\hat{D}_d &= (\hat{a}+d)(\hat{a}^\dagger+d^*), \end{aligned}$$

sendo $d \in \mathbb{C}$ um deslocamento qualquer no espaço de fase, obtemos

$$\langle\hat{a}_i\rangle = \langle\hat{a}_i^\dagger\rangle = 0, \qquad \langle\hat{a}_1^\dagger\hat{a}_1\rangle = \nu_1' + w_1^2r^2\alpha^2, \tag{5.63}$$

$$\langle\hat{a}_i^2\rangle = \langle\hat{a}_i^{\dagger 2}\rangle = 0, \qquad \langle\hat{a}_2^\dagger\hat{a}_2\rangle = \nu_2' + w_2^2r^2\alpha^2, \tag{5.64}$$

$$\langle\hat{a}_1\hat{a}_2^\dagger\rangle = \langle\hat{a}_1^\dagger\hat{a}_2\rangle = 0, \qquad \langle\hat{a}_1\hat{a}_2\rangle = \langle\hat{a}_1^\dagger\hat{a}_2^\dagger\rangle = w_1w_2r^2\alpha^2, \tag{5.65}$$

do que segue que $\hat{v}_Q$ tem valores esperados nulos dos operadores de quadratura e sua matriz de covariância é

$$\mathbf{\Gamma}(\hat{v}_Q) = \begin{pmatrix} (2(\nu_1' + w_1^2r^2\alpha^2)+1)\boldsymbol{I} & 2w_1w_2r^2\alpha^2\boldsymbol{Z} \\ 2w_1w_2r^2\alpha^2\boldsymbol{Z} & (2(\nu_2' + w_2^2r^2\alpha^2)+1)\boldsymbol{I} \end{pmatrix}, \tag{5.66}$$

e seus autovalores simpléticos ι_1 e ι_2 podem ser calculados pela Equação (5.38).

Afim de avaliar os resultados obtidos pela BMD, comparamos também com os valores de entropia da Espiã calculados pelo protocolo EB equivalente [87]. Analogamente ao protocolo BPSK utilizado como exemplo da Seção 5.1, o protocolo EB equivalente com constelação QPSK pode ser definido por meio de uma purificação adequada da mistura de Alice, um estado bipartido puro $|\Psi_4\rangle = \sum_{i=1}^4 \sqrt{\lambda_i}\,|\phi_i\rangle\,|\phi_i\rangle$, sendo

$$|\phi_i\rangle = \frac{e^{-\alpha^2/2}}{\sqrt{\lambda_i}} \sum_{n=0}^{\infty} (-1)^n \frac{\alpha^{4n+i}}{\sqrt{(4n+i)!}}\,|4n+i\rangle\,, \tag{5.67}$$

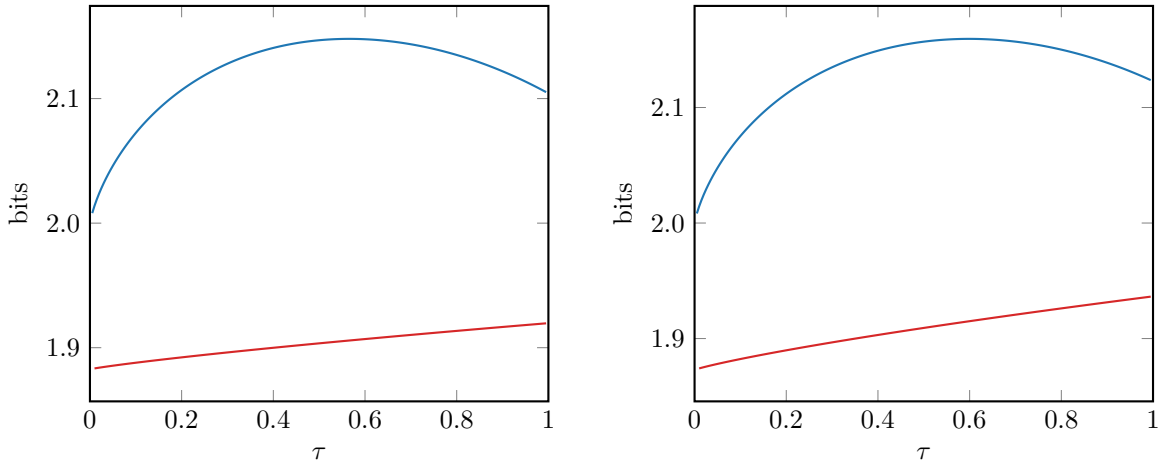
$$\lambda_i = \begin{cases} \frac{1}{2}e^{-\alpha^2}(\cosh\alpha^2 \pm \cos\alpha^2), \ i = \{0,2\} \\ \frac{1}{2}e^{-\alpha^2}(\sinh\alpha^2 \pm \sin\alpha^2), \ i = \{1,3\}, \end{cases} \tag{5.68}$$

cuja matriz de covariância é

$$\mathbf{\Gamma}_{\Psi_4} = \begin{pmatrix} (2\alpha^2+1)\boldsymbol{I} & z_4\boldsymbol{Z} \\ z_4\boldsymbol{Z} & (2\alpha^2+1)\boldsymbol{I} \end{pmatrix}, \qquad z_4 = 2\alpha^2 \sum_{k=0}^{3} \frac{\lambda_{k-1}^{3/2}}{\lambda_k^{1/2}}, \tag{5.69}$$

e a entropia obtida utilizando a hipótese gaussiana na matriz $\mathbf{\Gamma}_{\Psi_4}$ limita superiormente a entropia da espiã, i.e., $S(\hat{\rho}_{Eva}) = S(\hat{v}_Q) \leq S(\mathbf{\Gamma}(|\Psi_4\rangle\langle\Psi_4|))$.

Na Figura 25 traçamos as curvas das entropias $S(\hat{v}_Q^G)$ e $S(\mathbf{\Gamma}(|\Psi_4\rangle\langle\Psi_4|))$ para $\alpha = 1$ e $\bar{n} \in \{0.01, 0.02\}$ como uma função da transmitância τ. É possível ver que o limitante



(a) $\bar{n} = 0.01$. (b) $\bar{n} = 0.02$.

Figura 25 – Entropia de Eva em um cenário de protocolo DM-CVQKD com constelação QPSK calculada pelo protocolo EB equivalente ($\mathbf{\Gamma}_{\Psi_4}$, curva superior) e a decomposição BM usando o GET ($\mathbf{\Gamma}_{\upsilon_Q}$, curva inferior).

superior para $S(\hat{\upsilon}_Q)$ obtido pela BMD desenvolvida nessa seção se sai melhor que o limitante obtido pela hipótese gaussiana que é usualmente utilizada na literatura. Ainda, o valor da entropia do estado da espiã apresenta comportamento próximo ao linear (em função da transmitância) em contraste com a forte não linearidade do limitante calculado diretamente de $|\Psi_4\rangle\langle\Psi_4|$. É possível também notar que, para curtas distâncias ou baixa energia média de modulação, ou seja, $r, \alpha \to 0$, a matriz de covariância $\mathbf{\Gamma}(\hat{\upsilon}_Q)$ se aproxima de uma matriz diagonal em blocos com múltiplos da identidade, indicando um par de estados térmicos descorrelacionados. De fato, no limite $r \to 0$, $\boldsymbol{\beta}_i \to \mathbf{0}$ e $\hat{\upsilon}_Q = \hat{\rho}^{th}_{\nu_1'} \otimes \hat{\rho}^{th}_{\nu_2'}$ na Equação (5.62).

Por que não utilizar a matriz de Gram para misturas de estados térmicos?
É válido questionar o porquê de a entropia $S(\hat{\upsilon})$, que é uma mistura de estados quânticos, de acordo com o Teorema B.8. O motivo é que $\hat{\upsilon}$ é uma mistura de estados térmicos deslocados enquanto o Teorema B.8 garante a equivalência da entropia da matriz de Gram da mistura de estados puros. Ainda, o produto interno de Hilbert-Schmidt de estados gaussianos (Teorema B.22) não preserva a fase da sobreposição dos estados quânticos, de modo que a matriz normalizada de produtos internos para $\hat{\upsilon}$ não possui os mesmos autovalores de $\hat{\upsilon}$. Diferentemente, é possível utilizar a matriz de Gramm normalizada para misturas de estados térmicos, uma vez que esses são estados puros e o produto interno $\langle\alpha_1|\alpha_2\rangle$ preserva a fase da sobreposição dos estados (Equação (A.38)) .

Perspectivas sobre a Análise de Segurança

Nesse capítulo foi apresentado como a análise de segurança de um protocolo com modulação discreta é afetada pelo uso da hipótese gaussiana no protocolo EB equivalente de modo que a taxa de chave secreta gerada por um protocolo fica sempre limitada inferiormente pela taxa calculada como estado gaussiano equivalente e superiormente pelo protocolo com modulação gaussiana contínua. Foi apresentado como a decomposição de Bloch-Messiah pode ser aplicada para analisar o ataque de clonagem por emaranhamento, proporcionando uma nova perspectiva para análise do protocolo DM-CVQKD P&M sob a hipótese de ataques coletivos gaussianos com ruído térmico. No próximo capítulo, os limitantes superiores e inferiores para a taxa de chave real de um protocolo serão analisados com base na convergência de operadores de densidade e medidas de não gaussianidade de estados quânticos, tendo como consequência a convergência das taxas de chave secreta.

Capítulo 6

Convergência de Operadores e Segurança de Protocolos DM-CVQKD

Nas comunicações clássicas, o modelo de ruído aditivo gaussiano ocupa um lugar de grande importância, pois representa o ruído presente em diversos sistemas físicos para a transmissão de informação, como fibras ópticas e o espaço livre. A teoria da informação afirma que a maior taxa possível de transferência de informação (por uso do canal) é alcançada quando os símbolos de entrada do canal têm distribuição de probabilidade de acordo com uma curva gaussiana, conforme discutido no Capítulo 3. Contudo, por motivos de ordem prática na implementação dos sistemas de transmissão e compatibilidade com sistemas digitais de processamento da informação, os sistemas modernos de comunicação fazem uso de esquemas de modulação digital na transmissão de informação. Nesses esquemas, a taxa de transmissão de informação será necessariamente reduzida, mas, conforme os argumentos da Seção 3.1.1, é possível, em teoria, alcançar a capacidade do canal gaussiano por esquemas de modulação com constelações que convergem (em distribuição) para a gaussiana[1].

Para aplicações em protocolos CVQKD, observou-se nas Seções 3.2 e 3.3 que os esquemas de modulação que aproximam a capacidade do canal AWGN no caso clássico, quando aplicados à distribuição de chaves, também aproximam o desempenho de protocolos com modulação gaussiana contínua. Contudo, os resultados apresentados não fornecem uma justificativa formal dessa aparente convergência das taxas de chave secreta. O objetivo deste capítulo é então apresentar as condições para as quais a convergência é garantida. Mais precisamente, estaremos preocupados com as duas

[1]Para tal, é necessário um "casamento" entre o código de correção de erros e a arquitetura de formatação da constelação, como foi brevemente abordado na Seção 4.1.

seguintes desigualdades,

$$K(\hat{\rho}_{AB}) \geq K(\hat{\rho}_{AB_n}) \geq K(\rho^G_{AB_n}), \tag{6.1}$$

em que, para o canal quântico $\mathcal{N}$ utilizado por Alice e Bob para a transmissão dos estados quânticos, $\hat{\rho}_{AB} = (\mathbb{1} \otimes \mathcal{N})(|\nu\rangle\langle\nu|_{AB})$, sendo $|\nu\rangle$ um estado EPR, $\hat{\rho}_{AB_n}$ é uma purificação da constelação com $(n+1)^2$ estados (Equação (3.41)) e $\rho^G_{AB_n}$ é o estado gaussiano equivalente, os quais já foram previamente explorados na Seção 5.1. A desigualdade da direita corresponde ao que chamaremos de *lacuna de não gaussianidade* a qual sera visto que relaciona quantidade de "não gaussiandade" da constelação com a quantidade de chave secreta subestimada pelo uso da hipótese gaussiana para obter uma cota inferior para o protocolo com modulação discreta. A desigualdade à direita informa o quanto o protocolo com modulação não gaussiana está aquém do protocolo com modulação gaussiana, a lacuna de SKR já analisado previamente no Capítulo 3.

O restante do capítulo se organizará da seguinte forma. Na Seção 6.1, será apresentada uma introdução à teoria de recursos quânticos e a medida de não gaussianidade baseada na entropia relativa quântica. Os resultados desenvolvidos se concentram na convergência de operadores densidade e sua consequência para a não gaussianidade de misturas de estados coerentes. Na Seção 6.2, serão desenvolvidos resultados para a convergência de estados bipartidos que generalizam os resultados apresentados na Seção 6.1. Além disso, serão apresentadas resultados com cotas superiores para a distância entre os estados que descrevem os protocolos com modulação discreta e contínua gaussiana, e será discutido como essa aproximação se relaciona com a segurança incondicional dos protocolos.

6.1 Não Gaussianidade de Protocolos CVQKD

A Seção 5.1 tratou de discutir como, para um esquema de modulação com energia limitada, um protocolo DM-CVQKD tem seu desempenho limitado superiormente pelo protocolo com modulação gaussiana e inferiormente pelo protocolo EB equivalente que utiliza a hipótese gaussiana, Equação (5.10). Já no Capítulo 3, foi mostrado como o desempenho do protocolo UD-CVQKD pode ser aproximado por meio do aumento da cardinalidade de constelações unidimensionais formatadas geometricamente e probabilisticamente: a lacuna de SKR desaparece com o aumento da cardinalidade das constelações no cenário sem ruídos e com eficiência quântica unitária de detecção.

O problema que pretendemos abordar agora é o seguinte. A análise de segurança de protocolos QKD se torna mais simples quando feita a partir de um protocolo EB equivalente e, para o caso de um protocolo de DM-CVQKD, utilizar um protocolo

equivalente pode subestimar seu desempenho excessivamente devido à hipótese gaussiana, como apresentado na Figura 23b. Logo, de certa maneira, é natural supor que a diferença não nula e positiva $K(\hat{\rho}) - K(\rho_{AB}^{G})$ é resultante do caráter não gaussiano da constelação e é então razoável questionar: (i) como as medidas de não-gaussianidade desenvolvidas na teoria de recursos quânticos não-gaussianos podem ser utilizadas para auxiliar na análise de segurança de protocolos DM-CVQKD; (ii) quais medidas de não-gaussianidade fazem sentido operacionalmente no contexto de protocolos DM-CVQKD; e (iii) se é possível utilizar as ferramentas da nGQRT para investigar se o aumento da cardinalidade necessariamente implica na diminuição da não-gaussianidade de uma constelação, o que possibilitaria a utilização da hipótese gaussiana na análise de um protocolo CVQKD com modulação discreta sem comprometer seu desempenho esperado.

6.1.1 Uma Introdução à Teoria de Recursos Quânticos

Uma teoria de recursos quânticos (QRT, do inglês: *Quantum Resource Theory*), em um sentido mais amplo, investiga quais tarefas podem ser executadas quando existem restrições no conjunto de estados que podem ser preparados, chamados de *estados livres*, e de operações quânticas permitidas, chamadas de *operações livres*. Os objetos que não pertencem aos conjuntos de estados e operações livres são chamados de recursos [93].

Por exemplo, tome as formas geométricas que podem ser desenhadas com o uso de uma régua e um transferidor. O *conjunto de estados livres* é composto por polígonos, semicírculos, cones, etc., e as operações livres são o uso da régua e o uso do transferidor. Dessa forma, uma elipse é um "estado-recurso" e o uso de um compasso é uma "operação-recurso", uma vez que não é possível desenhar uma elipse apenas com uma régua e um transferidor. O uso de um compasso permite então compor um desenho que só é possível com o uso de uma elipse. Por outro lado, o acesso ao uso de uma elipse permite finalizar o desenho *simulando* a utilização de um compasso[2]. A definição formal de uma QRT é dada a seguir [93].

Definição 6.1. *Sejam A e B dois sistemas físicos quaisquer com os respectivos espaços de Hilbert $\mathcal{H}_A$ e $\mathcal{H}_B$ e $\mathcal{O}$ uma lei de associação que atribui aos sistemas A e B um conjunto único de operações CPTP $\mathcal{O}(A \to B) \subset \mathcal{Q}(A \to B)$. Seja $\mathcal{F}(A) := \mathcal{O}(\mathbb{C} \to \mathcal{H}_A)$ o conjunto de estados quânticos induzidos pelo mapeamento $\mathcal{O}$. Então, o par $\mathcal{R} = (\mathcal{F}, \mathcal{O})$ é uma QRT se as seguintes condições são atendidas:*

[2] O exemplo apresentado é uma adaptação do exemplo utilizado em [93, Sec. III].

(1) Para qualquer sistema A, o conjunto $\mathcal{O} := \mathcal{O}(A \to A)$ *contém o operador identidade,* $\mathcal{I}_A$.

(2) Para quaisquer sistemas A, B e C, se $\mathcal{E}_1 \in \mathcal{O}(A \to B)$ *e* $\mathcal{E}_2 \in \mathcal{O}(B \to C)$*, então* $\mathcal{E}_2 \circ \mathcal{E}_1 \in \mathcal{O}(A \to C)$.

Então, em uma QRT, o conjunto $\mathcal{F} \subset \mathcal{D}(\mathcal{H})$ define o conjunto de estados livres e os elementos pertencentes a $\mathcal{D}(\mathcal{H}) \setminus \mathcal{F}$ são os estados-recurso (ou recursos estáticos). Analogamente, os elementos pertencentes ao conjunto $\mathcal{O}(A \to B)$ são as operações livres da QRT e as operações-recurso são os elementos fora de $\mathcal{O}(A \to B)$, também chamados de recursos dinâmicos. Uma teoria de recursos quânticos irá então delimitar operacionalmente quais tarefas podem ser realizadas quando as operações ou estados são restringidos (ou ambos), e tais restrições podem ser oriundas das limitações técnicas dos dispositivos, regras de algum protocolo (ou jogo) ou simplesmente as leis da física [93]. Além disso, a condição (2) tem grande importância operacional, estabelecendo que *não existe composição de operações livres que irá mapear estados livres em estados-recurso*, o que é conhecido como *regra de ouro* das teorias de recursos quânticos: para quaisquer sistemas físicos A e B, se $\mathcal{E} \in \mathcal{O}(A \to B)$ e $\hat{\rho} \in \mathcal{F}(A)$, então $\mathcal{E}(\hat{\rho}) \in \mathcal{F}(B)$.

Transformação de Recursos

O conjunto $\mathcal{F}$ representa os estados que podem ser livremente preparados, dada a restrição operacional imposta pela aplicação que é representada pelo mapa $\mathcal{O}$ que define a QRT. Então, uma QRT deve especificar não apenas quais os tipos de operações podem ser realizadas com os estados (recursos estáticos), mas também por quais tipos de transformações os recursos dinâmicos podem passar. Essa generalização implica que, para uma QRT $\mathcal{R} = (\mathcal{O}, \mathcal{F})$, um recurso dinâmico $\mathcal{N} \in \mathcal{O}(A \to B)$ pode ser convertido para outro recurso dinâmico $\mathcal{M} \in \mathcal{O}(C \to D)$ por meio de um supercanal $\mathcal{J} \in \mathcal{L}(\mathcal{H}_A, \mathcal{H}_B) \to \mathcal{L}(\mathcal{H}_C, \mathcal{H}_D)$, de modo que $\mathcal{M} = \mathcal{J}(\mathcal{N})$. De fato, qualquer supercanal especificado da mesma forma que $\mathcal{M}$ pode ser realizado pelo uso de um sistema auxiliar E de modo que [94]

$$\mathcal{M} = \mathcal{J}_{pos}(\mathcal{N} \otimes \mathcal{I}_E)\mathcal{J}_{pre}, \tag{6.2}$$

sendo $\mathcal{J}_{pre} \in \mathcal{Q}(C \to AE)$ e $\mathcal{J}_{pos} \in \mathcal{Q}(BE \to D)$ mapas CPTP livres de pré- e pós-processamento. Então, a transformação entre recursos dinâmicos pode ser vista como a simulação de um canal específico pelo uso de recursos.

Exemplos importantes de interconversão entre recursos dinâmicos com o uso de sistemas auxiliares são os protocolos de teleporte quântico e codificação superdensa quântica. No primeiro, dois usos de um canal clássico discreto sem ruídos ($[c \to c]$)

simulam um uso de um canal quântico sem ruídos na transmissão de um bit quântico (*qubit*, do inglês: *quantum bit*), representado por $[q \to q]$, com o auxílio de um bit de emaranhamento (*ebit*, do inglês: *entangled bit*), representado por $[qq]$, e a conversão entre recursos é sumarizada na seguinte equação,

$$[qq] + 2[c \to c] \geq [q \to q]. \tag{6.3}$$

Já a codificação superdensa quântica simula dois usos de um canal clássico sem ruídos por meio de um uso de um canal quântico de um *qubit* e um *ebit*, de modo que

$$[qq] + [q \to q] \geq 2[c \to c]. \tag{6.4}$$

Na interconversão entre os recursos dinâmicos de canais clássicos e quânticos, um *ebit* é um recurso de um sistema auxiliar que é consumido para que a tarefa de processamento de informação seja realizada. Caso o *ebit* passe a ser um estado livre, o termo $[qq]$ pode ser removido das Equações (6.3) e (6.4), de modo que $[q \to q] = 2[c \to c]$.

Quantificando Recursos

Um dos aspectos das QRT's com forte apelo operacional é a possibilidade de quantificar um recurso físico, como apresentado nas equações de conversão de recursos em que precisamente um *ebit* e dois usos do canal clássico sem ruídos são consumidos para simular o canal quântico sem ruídos[3]. Portanto, funções de quantificação (ou de medida) de recursos quânticos podem ser definidas para diferentes QRT's, contanto que atendam a algumas propriedades matematicamente e operacionalmente razoáveis.

Consideremos uma função não-negativa $f : \mathcal{D}(\mathcal{H}) \to \mathbb{R}^+$ para um espaço de Hilbert $\mathcal{H}$ qualquer. Chamaremos f de uma *função de quantificação de recurso* (RQF, do inglês: *Resource Quantifying Function*) se atender aos seguintes axiomas.

Axioma 6.2 (Nulidade para estados-livres)**.** *Para um sistema físico A, se $\hat{\rho} \in \mathcal{F}(A)$, então $f(\hat{\rho}) = 0$.*

Axioma 6.3 (Monotonicidade)**.** *Uma RQF é um monótono para uma QRT se, para quaisquer $\mathcal{E} \in \mathcal{O}(A \to B)$ e $\hat{\rho} \in \mathcal{D}(A)$, têm-se que*

$$f(\hat{\rho}) \geq f(\mathcal{E}(\hat{\rho})). \tag{6.5}$$

Axioma 6.4 (Convexidade)**.** *Para quaisquer operadores de densidade $\{\hat{\rho}_i\}$ e distribuição de probabilidades $\{p_i\}$,*

$$f\left(\sum_i p_i \hat{\rho}_i\right) \leq \sum_i p_i f(\hat{\rho}_i). \tag{6.6}$$

[3]Os protocolos podem ser generalizados para admitir canais ruidosos.

Axioma 6.5 (Subaditividade)**.** *Para quaisquer* $\hat{\rho}, \hat{\sigma} \in \mathcal{D}(\mathcal{H})$*,*

$$f(\hat{\rho} \otimes \hat{\sigma}) \leq f(\hat{\rho}) + f(\hat{\sigma}). \tag{6.7}$$

Axioma 6.6 (Continuidade Assimptótica)**.** *Para quaisquer* $\hat{\rho}$ *e* $\hat{\sigma}$ *com suporte em* $\mathcal{H}$ *e uma constante* K*, seja* $\epsilon = \frac{1}{2}||\hat{\rho} - \hat{\sigma}||_1$ *e* $c(\epsilon)$ *alguma função em que* $\lim_{\epsilon \to 0} c(\epsilon) = 0$*, uma RQF* f *é assimptoticamente contínua se*

$$|f(\hat{\rho}) - f(\hat{\sigma})| \leq K\epsilon \log[\dim \mathcal{H} + c(\epsilon)]. \tag{6.8}$$

Os dois primeiros axiomas, nulidade para estados livres e monotonicidade, têm sentido intrínseco à teoria e são essenciais na especificação de uma RQF: um estado livre $\hat{\rho}$ não contém recurso, então $f(\hat{\rho})$ deve ter valor nulo, e uma operação livre não aumenta a quantidade de recurso em um estado, o que é uma generalização da regra de ouro das QRT's. Um aspecto interessante quanto ao axioma da nulidade para estados livres é que não é exigido que o contrário seja verdadeiro, ou seja, $f(\hat{\rho}) = 0 \not\Longrightarrow \hat{\rho} \in \mathcal{F}(A)$. Quando $f(\hat{\rho}) = 0 \iff \hat{\rho} \in \mathcal{F}(A)$, f é chamada de *fidedigna* para o recurso.

A convexidade de f surge como uma facilidade matemática (inclusive conveniente, permitindo o uso das ferramentas da análise convexa), mas seu sentido operacional depende da definição do processo que resulta em uma mistura de estados. A subaditividade de f é uma propriedade operacionalmente razoável, assim como a continuidade assintótica.

Desse modo, uma medida para a quantidade de recurso no contexto de uma QRT pode ser definida a partir de funções que atendam aos axiomas descritos. Uma forma de definir uma RQF para medir a quantidade de recurso de um estado quântico é utilizar uma função $d : \mathcal{D}(\mathcal{H}) \times \mathcal{D}(\mathcal{H}) \to \mathbb{R}^+$ que seja *contrativa* sob operações CPTP $\mathcal{E}$, ou seja, $d(\hat{\rho}, \hat{\sigma}) \geq d(\mathcal{E}(\hat{\rho}), \mathcal{E}(\hat{\sigma}))$, de modo que a monotonicidade esperada para uma RQF seja atendida e $d(\cdot, \cdot)$ seja uma medida de distância entre operadores de densidade. Então, $f_d(\hat{\rho})$ será a função de quantidade de recursos baseada na medida de distância d entre $\hat{\rho}$ e o conjunto dos estados livres $\mathcal{F}$,

$$f_d(\hat{\rho}) = \inf_{\hat{\sigma} \in \mathcal{F}} d(\hat{\rho}, \hat{\sigma}). \tag{6.9}$$

De modo análogo, é possível utilizar uma função entrópica, como a entropia relativa de Rényi quântica $D_\alpha(\hat{\rho}||\hat{\sigma})$ e a entropia relativa de von Neumann $S(\hat{\rho}||\hat{\sigma})$, no lugar de uma função de medida para estimar a quantidade de recurso em um estado ou então propor distâncias baseadas em entropias.

6.1.2 Teoria de Recursos Quânticos não Gaussianos

O conjunto $\mathcal{G}(\mathcal{H}_A) \subset \mathcal{D}(\mathcal{H}_A)$ composto pelos estados quânticos gaussianos do sistema de variáveis contínuas representado pelo espaço de Hilbert $\mathcal{H}_A$, juntamente com o conjunto de operações gaussianas $\mathcal{G}(\mathcal{H}_A \to \mathcal{H}_B) \subset \mathcal{L}(\mathcal{H}_A, \mathcal{H}_B)$, são peculiarmente importantes na óptica quântica, uma vez que estados e operações gaussianas são relativamente fáceis de serem realizados por meio de lasers, amplificadores, entre outros. Dessa forma, o "setor gaussiano" do espaço de Hilbert é o campo de trabalho sobre o qual a informação quântica gaussiana tem se desenvolvido, e os estados e operações gaussianas são os recursos necessários para a realização de diversos protocolos informacionais, como os protocolos CVQKD com modulação gaussiana de estados coerentes (GMCS, do inglês: *Gaussian Modulated Coherent State*), por exemplo.

Entretanto, em algumas tarefas de processamento da informação quântica, como destilação de emaranhamento [95, 96], correção de erros quânticos [97] e computação quântica universal [98, 99], estados e operações não gaussianas são recursos necessários ou desejados. Logo, uma teoria de recursos quânticos não gaussianos (nGQRT) surge naturalmente com $\mathcal{F} := \mathcal{G}(\mathcal{H}_A)$ e $\mathcal{O}(\mathcal{H}_A \to \mathcal{H}_B) := \mathcal{G}(\mathcal{H}_A \to \mathcal{H}_B)$ sendo os estados e operações livres e uma medida da quantidade de recurso de interesse deve medir a "não-gaussianidade" (nG) de um estado[4]. Um dos desafios impostos pela nGQRT é o fato de o conjunto dos estados gaussianos não ser um conjunto convexo, o que torna a nGQRT uma teoria não convexa de recursos.

Diversas medidas de não-gaussianidade (nG) foram propostas baseadas na distância para um *estado gaussiano de referência*. Para $\hat{\rho} \notin \mathcal{F}$, o estado de referência será o estado gaussiano equivalente $\hat{\rho}^G$ com os mesmo primeiro e segundo momentos estatísticos nos operadores canônicos que $\hat{\rho}$, e a quantidade de recurso de $\hat{\rho}$ é definida como a distância para seu equivalente gaussiano[5] $\delta_d(\hat{\rho}) = d(\hat{\rho}, \hat{\rho}^G)$, sendo d a distância de Hilbert-Schmidt $D_{HS}(\hat{\rho}, \hat{\sigma})$ [100] ou a fidelidade de Uhlmann [101], que na verdade é uma pseudo-distância. A distância de Hilbert-Schmidt é definida como

$$D_{HS}(\hat{\rho}, \hat{\sigma}) := \left(\frac{1}{2}\operatorname{tr}[(\hat{\rho} - \hat{\sigma})^2]\right)^{\frac{1}{2}} = \left(\frac{\mu(\hat{\rho}) + \mu(\hat{\sigma}) - 2\operatorname{tr}(\hat{\rho}\hat{\sigma})}{2}\right)^{\frac{1}{2}}, \tag{6.10}$$

em que $\mu(\hat{\rho}) = \operatorname{tr}(\hat{\rho}^2)$ é a pureza de $\hat{\rho}$. Então, as medidas de nG baseadas na distância de HS e na fidelidade de Uhlmann (que não é uma distância) serão, respectivamente,

$$\delta_{HS}(\hat{\rho}) = \frac{D^2_{HS}(\hat{\rho}, \hat{\rho}^G)}{\mu(\hat{\rho})}, \tag{6.11}$$

[4] Alguns trabalhos denotam a medida de nG de um estado como sendo uma medida do seu *caráter* não gaussiano ou o quanto um estado *falha* ao tentar se passar por um estado gaussiano.

[5] Aqui diferenciamos $\delta_d(\cdot)$ de uma FQR que é calculada de acordo com a Equação (6.9), que considera a menor distância de $\hat{\rho}$ para todo o conjunto de estados livres.

$$\delta_{UF}(\hat{\rho}) = -2\ln[F(\hat{\rho}, \hat{\rho}^G)]. \tag{6.12}$$

Outra forma de medir a quantidade de nG de um estado é através da entropia relativa de von Neumann (ou entropia relativa quântica, QRE, do inglês: *Quantum Relative Entropy*) a qual, assim como a fidelidade de Uhlmann, não é uma métrica propriamente dita (não é simétrica em suas entradas) mas atende aos requisitos esperados para uma RQF.

Definição 6.7 ([102])**.** *Seja $\hat{\sigma}$ um estado quântico arbitrário e $\hat{\sigma}^G$ seu equivalente gaussiano. A medida de não gaussianidade de $\hat{\sigma}$ baseada na entropia relativa quântica (nG QRE) é definida como*

$$\delta_{vN}(\hat{\rho}) = S(\hat{\rho}||\hat{\rho}^G). \tag{6.13}$$

Uma vez que na Equação (6.13), $\hat{\rho}$ e $\hat{\rho}^G$ têm a mesma matriz de covariância e $\log \hat{\rho}^G$ é um polinômio de segunda ordem nos operadores canônicos, tem-se que $\mathrm{tr}[(\hat{\rho}-\hat{\rho}^G)\log\hat{\rho}^G] = 0$ e ainda $\delta_{vN}(\hat{\sigma}) = S(\hat{\sigma}^G) - S(\hat{\sigma})$ [103]. Ainda mais, em [104] foi mostrado que a entropia relativa é uma medida exata de nG no sentido de que o estado gaussiano equivalente $\hat{\rho}^G$ é o estado gaussiano mais próximo (com relação à QRE) de $\hat{\rho}$, isto é,

$$\delta_{vN}(\hat{\rho}) = S(\hat{\rho}||\hat{\rho}^G) = \min_{\hat{\sigma}\in\mathcal{F}} S(\hat{\rho}||\hat{\sigma}) = f_{vN}(\hat{\rho}). \tag{6.14}$$

Dada a importância da quantidade δ_{vN} para o desenvolvimento da próxima seção, destacamos duas de suas propriedades.

Lema 6.8. *[102, Lema 01] $\delta_{vN}(\hat{\sigma})$ é uma quantidade não negativa com $0 \geq \delta_{vN}(\hat{\sigma}) \geq \infty$ e $\delta_{vN}(\hat{\sigma}) = 0$ se e somente se $\hat{\sigma}$ é um estado gaussiano.*

Lema 6.9. *[102, Lema 07] $\delta_{vN}(\hat{\sigma})$ decresce monotonicamente sob canais quânticos gaussianos, ou seja, $\delta_{vN}(\hat{\sigma}) \geq \delta_{vN}(\mathcal{N}(\hat{\sigma}))$ para todo $\mathcal{N} \in \mathcal{G}$.*

Destacamos ainda as medidas de nG baseadas na entropia Wehrl [105], que é a entropia diferencial da função Q-Husimi, a QRT desenvolvida em [106] em que tanto a não gaussianidade quanto a negatividade da função característica de Wigner são recursos, a depender da escolha do conjunto de estados livres, a QRT de *operações* não gaussianas [107] e a nGQRT com conjunto convexo de estados livres [99].

A seguir, serão desenvolvidos os resultados desta seção analisando o limitante inferior da taxa de chave secreta oriundo do estado gaussiano equivalente. Será definida a lacuna de não gaussianidade do protocolo DM-CVQKD, condições para a convergência de operadores de densidade e as consequências da convergência da entropia de von Neumann.

6.1.3 Não Gaussianidade de Protocolos DM-CVQKD[6]

Na Seção 3.2.1, o protocolo DM-CVQKD foi descrito de acordo com as implementações do tipo Prepara e Mede (com esquema de modulação unidimensional). A expressão geral da purificação do estado misto que representa uma constelação arbitrária do tipo QAM foi desenvolvida na Seção 3.3.1. Na Seção 3.3.2, foram calculados os limitantes inferiores para a taxa de chave secreta calculada a partir do estado gaussiano equivalente à purificação da constelação. O objetivo desta seção é exatamente avaliar o quão justa é a aproximação, definindo uma quantidade que chamaremos de "não gaussianidade do protocolo DM-CVQKD". Será visto também que essa quantidade é proporcional à medida de nG da constelação. Na discussão que segue, a menos que especificado, a medida de não gaussianidade do estado será a da Definição 6.7.

Antes de prosseguir, por conveniência, especificaremos novamente a estrutura do protocolo com modulação discreta, agora com interesse específico nas constelações do tipo QAM. Para tal, considere uma variável aleatória X_n, $n \geq 1$, com alfabeto complexo $\mathcal{X}_n$ e distribuição $Pr[X_n = x] = p_{X_n}(x)$. Por simplicidade e compatibilidade com os resultados anteriores, considere que $|\mathcal{X}_n| = (n+1)^2 = m^2 = N$. Sempre que estiver claro pelo contexto, utilizaremos $p(x)$ para a probabilidade *a priori* do símbolo x. Também será utilizada a notação $[N] = \{1, 2, \cdots, N\}$ e assumiremos que X_n é simétrica com relação à origem[7], ou seja, $p(x) = p(-x)\,\forall x \in \mathcal{X}_n$. O protocolo DM-CVQKD prepara e mede com m^2 estados *induzido* por X_n, e a detecção heteródina funciona da seguinte maneira.

(i) *Preparação dos estados* - Em cada rodada do protocolo, Alice sorteia uma realização x de X_n e prepara o estado $|x\rangle$. A constelação é representada pelo *ensemble* $\mathcal{A} = \{|x_k\rangle, p(x_k)\}_{k=1}^{N}$, que é a mistura $\hat{\rho}_{X_n} = \sum_{\alpha \in \mathcal{X}} p(x)\,|x\rangle\langle x|$. O registrador $\boldsymbol{X}'$ armazena a sequência de valores de amplitudes dos estados transmitidos.

(ii) *Transmissão e detecção quântica* - Alice envia os estados preparados por um canal quântico $\mathcal{N}_{A\to B}$, de modo que Bob observa a mistura $\hat{\rho}_B = \mathcal{N}_{A\to B}(\hat{\rho}_{X_n})$ e realiza a detecção heteródina nos estados recebidos, representada pelo operador $\mathcal{M}_{B\to Y}$. Os resultados das medições são armazenados no registrador $\boldsymbol{Y}'$.

(iii) *Sifting* - Após a conclusão de L rodadas, Alice e Bob concordam em um subconjunto $I_{test} \subset [L]$ de tamanho L' para compor o conjunto de teste a ser

[6]Os resultados apresentados nesta Seção foram submetidos para publicação na *IEEE Transactions on Communication*. Pre-print disponível em [108]

[7]Essa hipótese é feita sem perda de generalidade uma vez que as constelações que aproximam a capacidade do canal AWGN são usualmente simétricas [26].

utilizado na estimação de parâmetros. Os valores de $\boldsymbol{X}'$ e $\boldsymbol{Y}'$ indexados por I_{test} são anunciados publicamente e, em seguida, descartados. A chave bruta restante é indexada por $I_{key} = [L] \setminus I_{test}$ e representada por $\boldsymbol{X}$ e $\boldsymbol{Y}$ para Alice e Bob, respectivamente, com tamanho $l = L - L'$, sendo $L' \ll l$.

(iv) *Estimação de parâmetros* - Alice e Bob utilizam os conjuntos $\boldsymbol{X}'[I_{test}]$ e $\boldsymbol{Y}'[I_{test}]$ para estimar os parâmetros necessários para decidir se as chaves brutas podem gerar chaves seguras, calculando a taxa de chave secreta pela matriz de covariância reconstruída. Com base nos valores estimados, Alice e Bob decidem se é viável prosseguir com a geração da chave secreta ou se o protocolo deve ser abortado, retornando para o passo (i).

(v) *Reconciliação e amplificação de privacidade* - Caso os parâmetros estimados indiquem que é viável destilar uma chave secreta, Alice e Bob devem primeiro corrigir os erros entre suas sequências $\boldsymbol{X}$ e $\boldsymbol{Y}$, as chaves brutas, por meio de um protocolo de reconciliação[8]. Normalmente, um código corretor de erros é empregado nesse procedimento. A segunda tarefa será remover a quantidade de bits proporcional à informação obtida pela espiã, utilizando funções de *hashing*, que é a amplificação de privacidade.

A purificação desenvolvida na Equação (3.40), aplicada à mistura $\hat{\rho}_{X_n}$, permite o cálculo do limitante inferior para a chave secreta, usando as Equações (3.42), (3.44) e (3.51). Os parâmetros que devem ser escolhidos antes da comunicação quântica são a cardinalidade da constelação, m^2, e a energia média de modulação,

$$\langle \hat{n} \rangle = \mathrm{tr}(\hat{a}^\dagger \hat{a} \hat{\rho}_{X_n}) = \sum_{x \in \mathcal{X}_n} p(x)|x|^2 = \mathrm{Var}(X_n) = \bar{m}. \tag{6.15}$$

A seguir, será definida uma medida de não gaussianidade de um protocolo DM-CVQKD, conforme descrito acima, que representa a quantidade de taxa de chave secreta perdida na análise de segurança, como um tipo de penalidade devido ao uso de uma modulação não gaussiana. Posteriormente, algumas propriedades serão desenvolvidas e sua aplicação na análise de segurança do protocolo.

Definição 6.10 (Lacuna de não Gaussianidade do protocolo DM-CVQKD)**.** *Seja $\hat{\rho}_A = \hat{\rho}_{X_n}$ uma mistura não gaussiana de $N = (n+1)^2$ estados coerentes induzidos por uma variável aleatória X_n, $\hat{\rho}_{AA'} = |\Psi\rangle\langle\Psi|_{AA'}$ sua purificação, $\hat{\rho}_{AB} = (\mathbb{1}_A \otimes \mathcal{N}_{A' \to B})(|\Phi\rangle\langle\Phi|_{AA'})$*

[8] As sequências $\boldsymbol{X} \in \mathcal{X}_n^l$ e $\boldsymbol{Y} \in \mathbb{C}^l$ precisam ser convertidas em sequências binárias antes para que um código corretor de erros possa ser aplicado, mas desconsideraremos essa etapa na presente análise. A discussão sobre constelações com formatação probabilística e a adaptação da arquitetura PCS/PAS em sistemas QKD foi realizada na Seção 4.1.

o estado compartilhado por meio do canal quântico, e $\hat{\rho}_{AB}^{G}$ o equivalente gaussiano de $\hat{\rho}_{AB}$. Denote por $K(\hat{\rho}_{AB})$ e $K(\hat{\rho}_{AB}^{G})$ a taxa de chave secreta para $\hat{\rho}_{AB}$ e $\hat{\rho}_{AB}^{G}$, respectivamente, nas mesmas hipóteses (parâmetros do canal e energia média de modulação). A lacuna de não gaussianidade do protocolo definida por

$$\varepsilon_G(\hat{\rho}_{AB}) = K(\hat{\rho}_{AB}) - K(\hat{\rho}_{AB}^{G}), \tag{6.16}$$

representa a perda na taxa de chave secreta devido o limitante inferior calculado pelo modelo Gaussiano equivalente do estado bipartido compartilhado.

Lema 6.11. *A lacuna de não gaussianidade $\varepsilon_G(\hat{\rho}_{AB})$ é não negativa para qualquer protocolo DM-CVQKD sob ataques gaussianos coletivos.*

Demonstração. Devido ao teorema da extremalidade Gaussiana, $K(\hat{\rho}_{AB}) \geq K(\hat{\rho}_{AB}^{G})$. ■

Lema 6.12. *Para um protocolo DM-CVQKD cuja constelação é representada pelo operador de densidade $\hat{\rho}_A$, tem-se que*

$$\varepsilon_G(\hat{\rho}_{AB}) = \inf_{\mathcal{N}_{A'\to B}} \{\delta_{vN}(\mathcal{N}(\hat{\rho}_A))\} - D_{X_n}(\mathsf{snr}), \tag{6.17}$$

em que $\mathsf{snr} = \tau V_m/(1+\xi)$.

Demonstração. Desenvolvendo a expressão para $\varepsilon_G(\hat{\rho}_{AB})$, obtemos o seguinte resultado.

$$\varepsilon_G(\hat{\rho}_{AB}) = I(A;B) - \sup_{\mathcal{N}_{A'\to B}} \{\chi(B;E)\} - [I(A^G;B) - \chi(B^G;E)] \tag{6.18}$$

$$= \chi(B^G;E) - \sup_{\mathcal{N}_{A'\to B}} \{\chi(B;E)\} - [I(A^G;B) - I(A;B)]. \tag{6.19}$$

onde usamos o sobrescrito "G" para indicar que está sendo utilizado o respectivo sistema equivalente gaussiano. O supremo não aparece na quantidade de Holevo em relação ao sistema quântico Gaussiano equivalente porque o máximo é alcançado exatamente pelo canal gaussiano e $\chi(B^G;E)$ pode ser calculado a partir da matriz de covariância reconstruída com os parâmetros estimados. Como os canais quânticos considerados na otimização devem ser compatíveis com os dados observados, podemos afirmar que $\chi(B^G;E)$ depende apenas da escolha de $\hat{\rho}_{AB}$ e podemos descartar o supremo para este termo. O termo entre colchetes é exatamente igual à lacuna de capacidade $D_{X_N}(\mathsf{snr})$ de uma constelação de N pontos para o canal AWGN com snrdado por $\tau\tilde{V}_m/(1+\xi)$. A diferença das quantidades de Holevo pode ser desenvolvida como

$$\begin{aligned}\chi(B^G;E) - \sup_{\mathcal{N}_{A'\to B}} \chi(B;E) &= \inf_{\mathcal{N}_{A'\to B}} \left\{\chi(B^G;E) - \chi(B;E)\right\} \\ &= \inf_{\mathcal{N}_{A'\to B}} \left\{S(\rho_{AB}^G) - S(\rho_{AB}^G|B) - [S(\rho_{AB}) - S(\rho_{AB}|B)]\right\}\end{aligned} \tag{6.20}$$

$$= \inf_{\mathcal{N}_{A'\to B}} \delta_{vN}(\rho_{AB}) - [\delta_{vN}(\rho_{AB}) - \delta_{vN}(\rho_B)] \tag{6.21}$$

$$= \inf_{\mathcal{N}_{A'\to B}} \delta_{vN}(\rho_B). \tag{6.22}$$

onde na segunda igualdade usamos a identidade $S(\rho_{AB}^G|B) - S(\rho_{AB}|B) = \delta_{vN}(\rho_{AB}) - \delta_{vN}(\rho_B)$. Como $\hat{\rho}_B = \mathcal{N}(\hat{\rho}_A)$, segue que

$$\varepsilon_G(\hat{\rho}_{AB}) = \inf_{\mathcal{N}_{A'\to B}} \{\delta_{vN}(\mathcal{N}(\hat{\rho}_A))\} - D_{X_n}(\mathsf{snr}). \tag{6.23}$$

■

Vale destacar sobre a descrição equivalente da medida nG do protocolo DM-CVQKD que a diferença das informações do Holevo, que pode ser interpretada como a diferença entre o limite inferior obtido usando as propriedades extremas do estado gaussiano e o limite superior real (o supremo), é igual à menor medida de não gaussianidade do estado observado por Bob. Ou seja, em um protocolo DM-CVQKD, o canal quântico que dá à espiã a maior quantidade de informação sobre o sistema de Bob é o que faz o estado observado por Bob "mais gaussiano".

Do ponto de vista prático, é mais conveniente assumir o modelo gaussiano para os dados observados e usar a propriedade da extremalidade dos estados gaussianos para calcular a taxa de chave secreta do que calcular o supremo sobre a informação de Holevo. A penalidade do caminho mais fácil é ε_G. A seguir, mostramos como ε_G se torna desprezível com o aumento da cardinalidade das constelações adequadas usadas por Alice.

Convergência de Conjuntos de Estados Coerentes

Uma vez que a medida nG de um protocolo DM-CVQKD é limitada superiormente pela medida de nG do estado observado por Bob na saída do canal, é razoável questionar se existe algum tipo de constelação que Alice possa usar tal que o estado do lado de Bob é "Gaussiano o suficiente". Como a entropia de von Neumann é uma quantidade que é maximizada pelo estado quântico Gaussiano (para energia limitada), usamos como motivação as condições de alcance da capacidade do canal AWGN por medidas de probabilidade que convergem em distribuição para a distribuição normal e perguntamos: o que aconteceria com ε_G se tais constelações fossem usadas por Alice para transmitir estados coerentes? A seguir, serão apresentados alguns resultados de convergência para *ensembles* de estados coerentes induzidos por sequências convergentes de variáveis aleatórias. Começaremos pela definição de convergência de operadores limitados, que permite um resultado no limite da entropia de von Neumann de um estado quântico.

Definição 6.13 (Convergência Fraca de Operadores Limitados [109])**.** *Uma sequência de operadores limitados $\hat{A}_n$ em $\mathcal{B}(\mathcal{H})$ converge fracamente para $\hat{A}$ se* $\lim_{n\to\infty} \langle\psi|\hat{A}_n|\phi\rangle \to \langle\psi|\hat{A}|\phi\rangle$ *para cada* $\psi, \phi \in \mathcal{H}$.

Teorema 6.14 (Semicontinuidade à Esquerda da Entropia de von Neumann [109])**.** *A entropia quântica é semicontínua à esquerda no espaço operadores de densidade em $\mathcal{H}$. Seja $\{\hat{\sigma}_n\}$ uma sequência de operadores de densidade em $\mathcal{D}(\mathcal{H})$ convergindo para $\hat{\sigma}$. Então,*

$$S(\hat{\sigma}) \leq \liminf_{n\to\infty} S(\hat{\sigma}_n). \tag{6.24}$$

Para o próximo resultado, usamos a convergência na distribuição de uma variável aleatória em direção a uma distribuição normal para provar a convergência de operadores de densidade (adequados) em direção a um estado Gaussiano. Seja $\{X_n\}n \in \mathbb{N}$ uma sequência de variáveis aleatórias discretas com alfabetos $\mathcal{X}_n$ sobre o corpo complexo e distribuições P_{X_n}, $|\mathcal{X}_n| = (n+1)^2 = N$, $\mathbb{E}[X_n] = 0$ e $\mathbb{E}[X_n^2] = \bar{m}$. Denotamos por $\hat{\rho}_{X_n}$ o conjunto de estados coerentes induzidos pela variável aleatória X_n, ou seja, $\hat{\rho}_{X_n} = \sum_{i=1}^{N} p_{X_n}(x_i)\,|x_i\rangle\langle x_i|$. Analogamente, se X é uma variável aleatória contínua sobre o corpo dos complexos com distribuição $p_X(x)$, $\hat{\rho}_X = \int_{\mathbb{C}} p_X(x)\,|x\rangle\langle x|\,\mathrm{d}^2x$.

Teorema 6.15. *Se $X_G \sim \mathbb{C}\mathcal{N}(0,\bar{m})$ e $\{X_n\}_{n\in\mathbb{N}}$ é uma sequência de variáveis aleatórias tal que $X_n \xrightarrow{\mathcal{D}} X_G$ então $\hat{\rho}_{X_n} \to \hat{\rho}_{X_G} = \hat{\rho}^{th}(\bar{m})$.*

Demonstração. Primeiro, notamos que $\hat{\rho}^{th}(\bar{m}) = \hat{\rho}_{X_G}$ devido à representação de Glauber-Surdashan de um estado térmico:

$$\hat{\rho}^{th}(\bar{m}) = \frac{1}{\pi\bar{m}} \int_{\mathbb{C}} \exp\left\{\frac{-|x|^2}{\bar{m}}\right\} |x\rangle\langle x|\,\mathrm{d}^2x\,. \tag{6.25}$$

Para provar a convergência, tomemos $|\phi\rangle, |\psi\rangle \in \mathcal{H}$ arbitrários. Da definição de $\hat{\rho}_{X_n}$, temos que

$$\langle\psi|\hat{\rho}_{X_n}|\phi\rangle = \langle\psi|\left(\sum_{i=1}^{n} p_{X_n}(x_i)\,|x_i\rangle\langle x_i|\right)|\phi\rangle = \sum_{i=1}^{n} p_{X_n}(x_i)\,\langle\psi|x_i\rangle\cdot\langle x_i|\phi\rangle\,, \tag{6.26}$$

para o qual, assumindo sem perda de generalidade que $\phi = \sum_{j=0}^{\infty}\phi_j\,|j\rangle$ e $\psi = \sum_{k=0}^{\infty}\psi_k\,|k\rangle$ são as respectivas expansões dos estados na base de Fock, obtemos

$$\langle\psi|x_i\rangle = e^{-|x_i|^2/2}\sum_{j=0}^{\infty}\psi_j^*\frac{x_i^j}{\sqrt{j!}}, \qquad \langle x_i|\phi\rangle = e^{-|x_i|^2/2}\sum_{k=0}^{\infty}\phi_k\frac{(x_i^*)^k}{\sqrt{k!}}. \tag{6.27}$$

A junção das expressões resulta em

$$\langle\psi|\hat{\rho}_{X_n}|\phi\rangle = \sum_{i=1}^{n} p_{X_n}(x_i)\left[e^{-|x_i|^2}\sum_{j,k=0}^{\infty}\psi_j^*\phi_k\frac{x_i^j(x_i^*)^k}{\sqrt{j!k!}}\right]. \tag{6.28}$$

Agora, pegue a representação de Glauber-Surdashan de um estado térmico $\hat{\rho}^{th}(\bar{m})$ e calcule $\langle\psi|\hat{\rho}^{th}(\bar{m})|\phi\rangle$:

$$\langle\psi|\hat{\rho}^{th}(\bar{m})|\phi\rangle = \sum_{j=0}^{\infty} \psi_j^* \langle j| \left[\int_{\mathbb{C}} p(x) |x\rangle\langle x| \, \mathrm{d}^2x\right] \sum_{k=0}^{\infty} \phi_k |k\rangle \tag{6.29}$$

$$= \int_{\mathbb{C}} p(x) \left[\sum_{j,k=0}^{\infty} \psi_j^* \phi_k \langle j|x\rangle \langle x|k\rangle\right] \mathrm{d}^2x \tag{6.30}$$

$$= \int_{\mathbb{C}} p(x) \left[e^{-|x|^2} \sum_{j,k=0}^{\infty} \psi_j^* \phi_k \frac{x^j (x^*)^k}{\sqrt{j!k!}}\right] \mathrm{d}^2x \,, \tag{6.31}$$

Agora, como $X_n \to X_G$, tem-se que[9] $\mathcal{L}(X_n) \to \mathcal{L}(X_G)$ [68] e comparando (6.28) e (6.31), $\langle\psi|\hat{\rho}_{X_n}|\phi\rangle \to \langle\psi|\hat{\rho}^{th}(\bar{m})|\phi\rangle$. Como $|\psi\rangle$ e $|\phi\rangle$ foram escolhidos arbitrariamente, concluímos que se $X_n \to X_G$ então $\hat{\rho}_{X_n} \to \hat{\rho}_{X_G} = \hat{\rho}^{th}(\bar{m})$. ■

Destaque 6.16. *Como a sequência $\{X_n\}_{n\in\mathbb{N}}$ foi escolhida de forma que cada elemento tenha o mesmo primeiro e segundo momentos, tem-se $\hat{\rho}^G_{X_n} = \hat{\rho}^G_{X_G} = \hat{\rho}_{X_G} = \hat{\rho}^{th}(\bar{m})$.*

Com a convergência dos operadores de densidade para um estado quântico gaussiano definido, podemos agora explorar a convergência da medida não gaussiana.

Corolário 6.17. *Se $X_n \xrightarrow{\mathcal{D}} X_G$ então $\lim_{n\to\infty} \delta_{vN}(\hat{\rho}_{X_n}) = 0$.*

Demonstração. Dos Teoremas 6.14 e 6.15, temos que $S(\hat{\rho}_{X_G}) \leq \liminf_{n\to\infty} S(\hat{\rho}_{X_n})$ e do teorema da extremalidade Gaussiana, $S(\hat{\rho}_{X_G}) \geq S(\hat{\rho}_{X_n})$. Então, $\lim_{n\to\infty} S(\hat{\rho}_{X_n}) = S(\hat{\rho}_{X_G})$. Como $\delta_{vN}(\hat{\rho}_{X_n}) = S(\hat{\rho}^G_{X_n}) - S(\hat{\rho}_{X_n})$ e $\hat{\rho}^G_{X_n} = \hat{\rho}_{X_G}$, então $\lim_{n\to\infty} \delta_{vN}(\hat{\rho}_{X_n}) = 0$. ■

Conforme a definição, $\varepsilon_G(\hat{\rho}_{AB})$ representa a perda de SKR como consequência de assumir um modelo gaussiano para os dados observados por Alice e Bob. A quantidade de SKR perdida é proporcional à medida de nG do estado de Bob e, como o canal que conecta Alice e Bob é desconhecido, envolve uma otimização considerando todos os canais quânticos compatíveis com as estatísticas observadas, geralmente a transmitância τ e o excesso de ruído ξ. O seguinte resultado afirma que $\varepsilon_G(\hat{\rho}_{AB})$ torna-se insignificante à medida que a cardinalidade cresce se o formato da constelação for escolhido corretamente.

Corolário 6.18. *Se $X_n \xrightarrow{\mathcal{D}} X_G$ Então $\varepsilon_G(\hat{\rho}_{AB}) \to 0$.*

Demonstração. Do Lema 6.12, a convergência de duas quantidades precisa ser analisada. Para a lacuna de capacidade, temos que $D_{X_n}(\mathsf{snr}) \to 0$ desde $X_n \xrightarrow{\mathcal{D}} X_G$

[9] Aqui, se A é uma variável aleatória, $\mathcal{L}(A)$ representa a lei de A.

independentemente do canal quântico considerado porque deve corresponder às estatísticas observadas durante a estimativa de parâmetros. Agora devemos mostrar que $\inf_{\mathcal{N}_{A'\to B}}\{\delta_{vN}(\mathcal{N}(\hat{\rho}_A))\}\to 0$. Seja $\hat{\rho}$ um estado quântico arbitrário, $\mathcal{N}^*$ o canal quântico para o qual o ínfimo é alcançado e tome um canal quântico gaussiano arbitrário $\mathcal{N}$, ambos compatíveis com os parâmetros estimados. Então, usando a Lema 6.9 de δ_{vN},

$$\delta_{vN}(\hat{\rho}_A)\geq\delta_{vN}(\mathcal{N}(\hat{\rho}_A))\geq\delta_{vN}(\mathcal{N}^*(\hat{\rho}_A)). \tag{6.32}$$

Fazendo $\hat{\rho}_A=\hat{\rho}_{X_N}$ e escolhendo uma sequência tal que $X_n\xrightarrow{\mathcal{D}}X_G$, Corolário 6.17 garante que

$$\lim_{n\to\infty}\delta_{vN}(\mathcal{N}^*(\hat{\rho}_{X_N}))\leq\lim_{n\to\infty}\delta_{vN}(\hat{\rho}_{X_n})=0. \tag{6.33}$$

Então, $\varepsilon_G(\hat{\rho}_{AB})\to 0$. ■

A interpretação operacional é que se Alice escolhe $X_i\in\{X_n\}$ para definir as amplitudes e distribuição de probabilidade de seus estados coerentes (a constelação) e tal sequência de variáveis aleatórias converge para uma distribuição normal, ela e Bob podem seguramente reconstruir a matriz de covariância para o protocolo baseado em emaranhamento equivalente e saber que a quantidade de taxa de chave secreta perdida devido ao limitante inferior se torna pequena se a cardinalidade da constelação for grande o suficiente.

Resultados Numéricos

Uma vez que $\delta_{vN}\geq\varepsilon_G$, na Figura 26 plotamos os valores de nG das constelações de estados coerentes com formas GQ e RW com energia média de modulação fixa $\bar{m}=2.5$. A queda de δ_{vN} com o tamanho da constelação é semelhante à lacuna de capacidade Definição 3.1 na Figura 15 – a constelação RW funciona melhor que a GQ para constelações menores, com ponto de inflexão em $N=144$. Além disso, é possível observar que, analogamente à lacuna de capacidade clássica, a QRE-nG decresce exponencialmente, significando que a mistura não gaussiana de estados coerentes converge para o estado equivalente gaussiano com velocidade exponencial.

O gráfico na Figura 26 mostra como δ_{vN} diminui sob a ação de um canal quântico (fibra ótica, caracterizado pela transmitância e ruído de excesso). A curva superior em azul corresponde à medida de nG da constelação na entrada do canal e as linhas inferiores são os valores de nG do estado na saída do canal para transmitância fixa $\tau=0.5$ e $\bar{n}=0,0.2,0.4$, respectivamente. Os resultados indicam que a nG do estado de saída do canal é monotônica em relação à transmitância do canal e ao excesso de ruído, também observado na Figura 27, onde plotamos δ_{vN} em função da distância $D=-100\cdot\log_{10}(\tau)$ e na Figura 27 em função da energia média de modulação para os dois formatos de

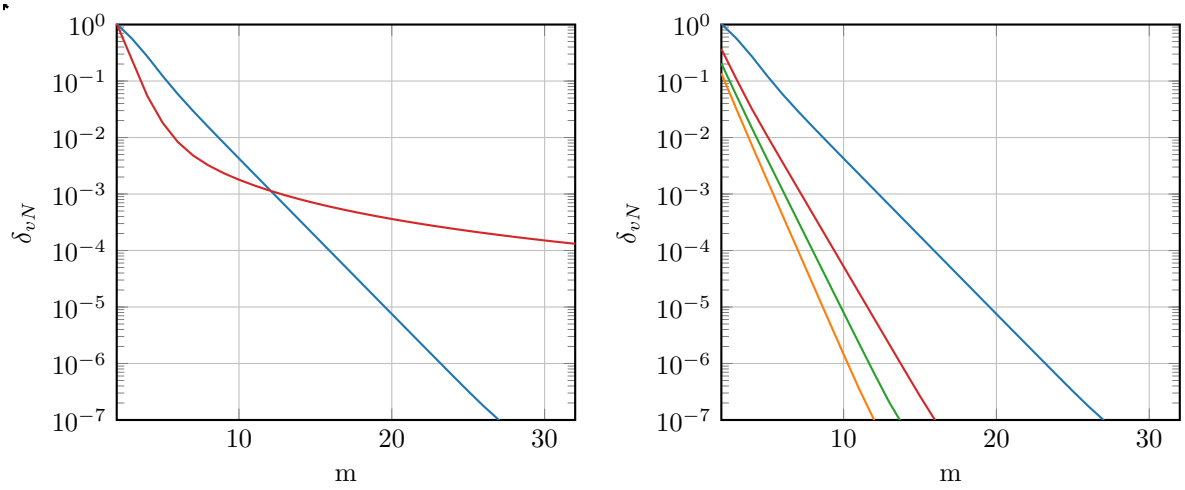


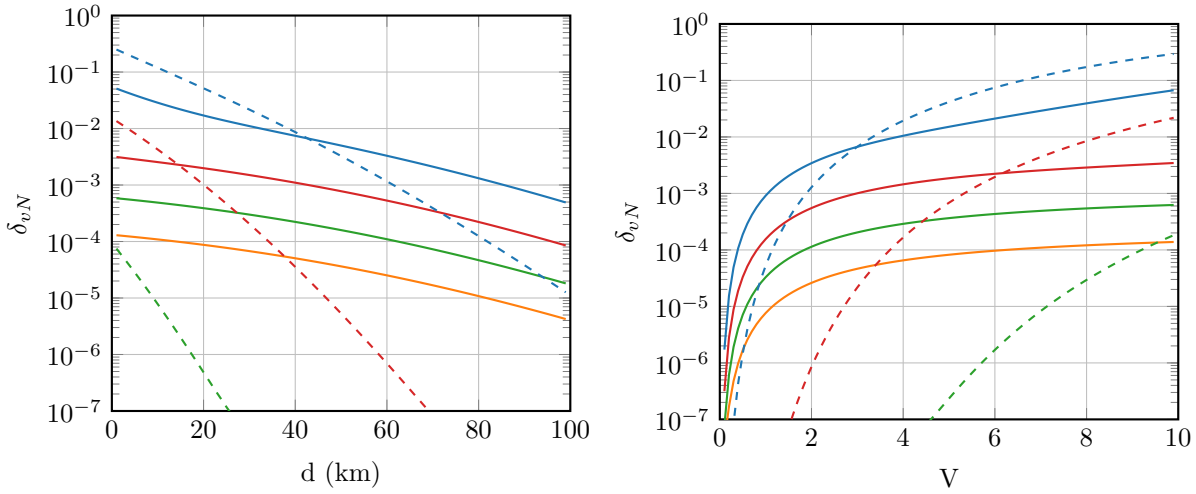
Figura 26 – (a) Valores da QRE-nG para as constelações RW-QAM (curva azul) e GQ-QAM (curva vermelha) com pontos $N = m^2$ e energia média de modulação $\bar{m} = 2.5$. (b) Valores da QRE-nG para a constelação GQ-QAM com $N = m^2$ pontos sob um canal de perdas térmicas com transmitância fixa ($\tau = 0.5$). A linha superior (azul) corresponde aos valores de nG da constelação na entrada canal e nas três linhas abaixo correspondem aos valores de ruído térmico $\bar{n} = \{0, 0.2, 0.4\}$.

constelação estudados com tamanhos 16, 64, 256 e 1024. Em ambos os gráficos vemos consonância com os resultados observados na Figura 26, em que o melhor formato de constelação depende da distância e energia de modulação: em geral, as constelações GQ têm melhor desempenho para distâncias maiores, bem como para constelações maiores; a constelação 256GQ-QAM apresenta menores valores de nG do que a 256RW-QAM para cada distância e variação de modulação considerada.

É relevante notar que a medida de nG diminui rapidamente à medida que o tamanho da constelação cresce, mesmo quando nG é calculada na saída do canal quântico. Além disso, a medida von Neumann nG aumenta com a energia média da constelação, o que é esperado, pois fica mais fácil distinguir entre os estados em um conjunto de estados coerentes distantes quando esses estados estão mais distantes (em uma imagem do espaço de fase).

6.1.4 Canais não Gaussianos: O Processo de Difusão de Fase

A decoerência é o resultado de processos ruidosos oriundos do acoplamento do sistema principal com o ambiente externo, onde os estados quânticos perdem suas características que são "fundamentalmente quânticas" – os estados com decoerência total se reduzem a misturas de estados ortogonais que podem ser perfeitamente distinguidos.



(a) (b)

Figura 27 – (a) Valores do QRE-nG para as constelações RW-QAM (cuvas sólidas) e GQ-QAM (cuvas tracejadas) Para o canal com $\bar{n} = 0.1$ e transmitância $\tau = 10^{-0.01d}$, d sendo a distância em quilômetros. De cima para baixo, os tamanhos das constelações são 16, 64, 256 e 1024, respectivamente. (b) Valores do QRE-nG para as constelações RW-QAM (cuvas sólidas) e GQ-QAM (cuvas tracejadas) em função da energia média de modulação ruído térmico fixo $\bar{n} = 0.1$ e $d = 50$km. De cima para baixo, os tamanhos das constelações são 16, 64, 256 e 1024, respectivamente.

Alguns processos de sistema aberto resultam em mudanças aleatórias nas fases relativas dos estados que estão em superposição no sistema quântico principal. Tais flutuações das fases relativas resultam na perda de coerência e são chamadas de amortecimento de fase ou difusão de fase [110].

A evolução de um sistema de um modo sob tal processo pode ser descrita pela equação mestra [111, 112]

$$\frac{\mathrm{d}}{\mathrm{d}t}\hat{\rho} = \Gamma\mathcal{L}[\hat{a}^\dagger\hat{a}]\hat{\rho}, \tag{6.34}$$

emq que $\mathcal{L}[\hat{O}]\hat{\rho} = 2\hat{O}^\dagger\hat{\rho}\hat{O} - \hat{O}^\dagger\hat{O}\hat{\rho} - \hat{\rho}\hat{O}^\dagger\hat{O}$, ou como o hamiltoniano de um oscilador harmônico aberto para um ambiente de N modos [110]

$$H = \hbar\omega\hat{a}^\dagger\hat{a} + \hbar\sum_{i=1}^{N}\omega_i\hat{a}_i^\dagger\hat{a}_i + \hbar\sum_{i=1}^{N}\chi_i\hat{a}^\dagger\hat{a}(\hat{a}_i + \hat{a}_i^\dagger), \tag{6.35}$$

onde $\hat{a}$ e $\hat{a}^\dagger$ são os operadores de aniquilação e criação do sistema principal com frequência ω e $\hat{a}_i$ e $\hat{a}_i^\dagger$ referem-se ao i-ésimo modo do ambiente com frequência ω_i. A quantidade χ_i representa um parâmetro de acoplamento entre o sistema principal e o i-ésimo modo do ambiente.

Essa evolução não gaussiana de um estado quântico é uma importante fonte de ruído em enlaces de comunicação óptica. Seu conjunto de operadores Krauss $\{P_k(t)\}$,

$0 \leq k \leq \infty$ possui elementos

$$P_k(t) = \sum_{n=0}^{\infty} e^{-\frac{1}{2}n^2\lambda^2} \sqrt{\frac{(n^2\lambda^2)^k}{k!}} \, |n\rangle\langle n| \tag{6.36}$$

onde $\lambda = t\sqrt{\Lambda}$ e $\Lambda = \sum_i \chi_i^2 \sqrt{1 - e^{-n^2\lambda^2}}$.

Vamos primeiro analisar a evolução da difusão de fase de um estado térmico com número médio de fótons $\bar{n}$, $\hat{\rho}^{th}(\bar{n})$:

$$\begin{aligned}
\sum_{k=0}^{\infty} P_k(t)\hat{\rho}^{th}(\bar{n})P_k^{\dagger}(t) = &\sum_{k,n=0}^{\infty} e^{-\frac{1}{2}n^2\lambda^2} \sqrt{\frac{(n^2\lambda^2)^k}{k!}} \, |n\rangle\langle n| \cdot \sum_{m=0}^{\infty} \frac{\bar{n}^m}{(\bar{n}+1)^{m+1}} \, |m\rangle\langle m| \times \\
&\sum_{l=0}^{\infty} e^{-\frac{1}{2}l^2\lambda^2} \sqrt{\frac{(l^2\lambda^2)^k}{k!}} \, |l\rangle\langle l| \,, \qquad (6.37) \\
= &\sum_{k,l,m,n=0}^{\infty} \frac{e^{-\frac{1}{2}n^2\lambda^2} e^{-\frac{1}{2}l^2\lambda^2} \bar{n}^m \sqrt{(n^2\lambda^2)^k (l^2\lambda^2)^k}}{k!(\bar{n}+1)^{m+1}} \, |n\rangle \, \langle n|m\rangle \, \langle m|l\rangle \, \langle l| \qquad (6.38) \\
= &\sum_{k=0}^{\infty}\sum_{n=0}^{\infty} e^{-n^2\lambda^2} \frac{(n^2\lambda^2)^k}{k!} \frac{\bar{n}^n}{(\bar{n}+1)^{n+1}} \, |n\rangle\langle n| \qquad (6.39) \\
= &\sum_{n=0}^{\infty} e^{-n^2\lambda^2} \sum_{k=0}^{\infty} \left[\frac{(n^2\lambda^2)^k}{k!}\right] \frac{\bar{n}^n}{(\bar{n}+1)^{n+1}} \, |n\rangle\langle n| \qquad (6.40) \\
= &\sum_{n=0}^{\infty} \frac{\bar{n}^n}{(\bar{n}+1)^{n+1}} \, |n\rangle\langle n| = \hat{\rho}^{th}(\bar{n}) \qquad (6.41)
\end{aligned}$$

Então, os estados térmicos são invariantes ao processo de difusão de fase. Este comportamento não está presente em todos os estados gaussianos, uma vez que para um estado coerente $|\alpha\rangle$ com $\alpha = (q + ip)/2$,

$$\begin{aligned}
\mathcal{N}_{\Delta}(|\alpha\rangle\langle\alpha|) = &e^{-|\alpha|^2} \sum_{m,n=0}^{\infty} \exp\{-\Delta^2(n-m)^2\} \\
&\times \frac{\alpha^n \alpha^{*m}}{\sqrt{n!m!}} \, |n\rangle\langle m| \qquad (6.42)
\end{aligned}$$

é um estado misto não gaussiano com $\Delta = \lambda^2/2$. Os valores esperados das combinações dos operadores bosônicos para o estado da Equação (6.42) são

$$\begin{aligned}
&\langle\hat{a}\rangle = e^{-\Delta^2}\alpha, && \langle\hat{a}^{\dagger}\rangle = e^{-\Delta^2}\alpha^*, && \langle\hat{a}^2\rangle = e^{-4\Delta^2}\alpha^2, \\
&\langle\hat{a}^{\dagger 2}\rangle = e^{-4\Delta^2}\alpha^{*2}, && \langle\hat{a}^{\dagger}\hat{a}\rangle = e^{-\Delta^2}|\alpha|^2,
\end{aligned}$$

resultando no vetor de médias

$$\bar{\boldsymbol{x}} = \begin{pmatrix} \langle\hat{q}\rangle \\ \langle\hat{p}\rangle \end{pmatrix} = \begin{pmatrix} q \cdot e^{-\Delta^2} \\ p \cdot e^{-\Delta^2} \end{pmatrix}, \tag{6.43}$$

e os elementos da matriz de covariância são

$$[\mathbf{\Gamma}]_{1,1} = 1 + 2|\alpha|e^{-\Delta^2} + e^{-4\Delta^2}(\alpha^2 + \alpha^{*2}) - q^2 e^{-2\Delta^2}, \tag{6.44}$$

$$[\mathbf{\Gamma}]_{2,2} = 1 + 2|\alpha|e^{-\Delta^2} - e^{-4\Delta^2}(\alpha^2 + \alpha^{*2}) - p^2 e^{-2\Delta^2}, \tag{6.45}$$

$$[\mathbf{\Gamma}]_{1,2} = [\mathbf{\Gamma}]_{2,1} = qp(e^{-4\Delta^2} - e^{-2\Delta^2}). \tag{6.46}$$

Em contraste com os estados térmicos, os estados coerentes sofrem de decoerência em uma evolução de difusão de fase, com os elementos fora da diagonal do operador de densidade sendo mais afetados à medida que o parâmetro de ruído Δ se torna maior. Além disso, o vetor de médias e a matriz de covariância também mudam com Δ.

Agora, considere misturas de estados coerentes, especificamente aqueles que representam constelações em um esquema de modulação digital, como $\hat{\rho} = \sum_i p_i \, |\alpha_i\rangle\langle\alpha_i|$, e denotamos $\hat{\rho}_\Delta = \mathcal{N}_\Delta(\hat{\rho})$. Devido à linearidade do canal, usamos (6.42) diretamente e temos

$$\hat{\rho}_\Delta = \sum_{m,n=0}^{\infty} e^{-\Delta^2(n-m)^2} \sum_{i=0}^{N} p_i e^{-|\alpha_i|^2} \frac{\alpha_i^n \alpha_i^{*m}}{\sqrt{n!m!}} \, |n\rangle\langle m| \tag{6.47}$$

Devido à linearidade da transformação, a mistura resultante também será não gaussiana. Os valores esperados dos operadores bosônicos resultam em

$$\mathrm{tr}(\hat{a}\hat{\rho}_\Delta) = \sum_{i=1}^{N} \Theta_i \alpha_i \qquad\qquad \mathrm{tr}(\hat{a}^\dagger \hat{\rho}_\Delta) = \sum_{i=1}^{N} \Theta_i \alpha_i^*, \tag{6.48}$$

onde fizemos $\Theta_i = e^{-\Delta^2} p_i e^{-|\alpha_i|^2} \cosh |\alpha_i|^2$, o que resulta em

$$\mathrm{tr}(\hat{q}\hat{\rho}_\Delta) = \mathrm{tr}(\hat{p}\hat{\rho}_\Delta) = 0, \tag{6.49}$$

indicando que o processo de difusão de fase não modifica o primeiro momento do estado misto inicial. Para o segundo momento, temos as seguintes quantidades,

$$\mathrm{tr}(\hat{a}^2\hat{\rho}_\Delta) = e^{-4\Delta^2} \sum_{i=1}^{N} p_i \alpha_i^2 \tag{6.50}$$

$$\mathrm{tr}(\hat{a}^{\dagger 2}\hat{\rho}_\Delta) = e^{-4\Delta^2} \sum_{i=1}^{N} p_i \alpha_i^{*2} \tag{6.51}$$

$$\mathrm{tr}(\hat{a}^\dagger \hat{a}\hat{\rho}_\Delta) = \mathrm{tr}(\hat{a}^\dagger \hat{a}\hat{\rho}) = \sum_{i=1}^{N} p_i |\alpha_i|^2, \tag{6.52}$$

o que resulta em

$$[\mathbf{\Gamma}]_{1,1} = [\mathbf{\Gamma}]_{2,2} = 1 + 2\sum_{i=1}^{N} p_i |\alpha_i|^2 \tag{6.53}$$

$$[\mathbf{\Gamma}]_{1,2} = [\mathbf{\Gamma}]_{2,1} = 0 \tag{6.54}$$

de modo que $\mathbf{\Gamma}(\hat{\rho}_\Delta) = \mathbf{\Gamma}(\hat{\rho})$. No que foi exposto, o canal de difusão de fase, por não ser gaussiano, não necessariamente mapeia estados gaussianos em estados gaussianos, mas há casos em que isso acontece: estados térmicos são invariantes, em oposição a estados coerentes. Curiosamente, misturas "simétricas" (com relação à origem no espaço de fase) de estados coerentes têm os primeiros e segundos momentos estatísticos preservados durante o processo de difusão de fase. Podemos então assumir que existe um conjunto de estados quânticos (misturas convexas de estados coerentes) cujos primeiros e segundos momentos estatísticos são invariantes para algumas evoluções não gaussianas do sistema.

Processos não Gaussianos que Preservam a Monotonicidade Decrescente da QRE-nG

Na demonstração do Corolário 6.18, foi observado que, dado um estado quântico $\hat{\rho}$, é possível que existam canais quânticos não gaussianos tais que $\delta_{vN}(\hat{\rho}) \geq \delta_{vN}(\mathcal{N}(\hat{\rho}))$, ou pelo menos aqueles para os quais a medida QRE-nG não aumenta. Em outras palavras, a propriedade da monotonicidade da QRE-nG pode ser estendida a algum conjunto de canais quânticos além do setor gaussiano, mesmo que seja restrita a algum conjunto específico de estados quânticos. O objetivo desta seção é descrever as condições para as quais um canal quântico nG mantém a propriedade monotônica da QRE-nG e como tais canais podem ser úteis na descrição dos canais quânticos relevantes para protocolos DM-CVQKD. Vamos iniciar provando o seguinte lema.

Lema 6.19. *Seja $\mathcal{N}$ um canal quântico, $\hat{\rho}$ um estado quântico arbitrário e defina*

$$\Delta(\mathcal{N}, \hat{\rho}) = \mathrm{tr}[\mathcal{N}(\hat{\rho})(\log \mathcal{N}(\hat{\rho})^G - \log \mathcal{N}(\hat{\rho}^G))]. \tag{6.55}$$

Se $\mathcal{N}$ é Gaussiano, então $\Delta(\mathcal{N}, \hat{\rho}) = 0$ para qualquer estado quântico $\hat{\rho}$.

Demonstração. Se $\mathcal{N}$ é um canal gaussiano e $\mathbf{\Gamma}$ é a matriz de covariância de um estado quântico arbitrário $\hat{\rho}$, então $\mathbf{\Gamma}(\hat{\rho}) = \mathbf{\Gamma}(\hat{\rho}^G)$ e $\mathbf{\Gamma} \xrightarrow{\mathcal{N}} \mathbf{\Gamma}'$. Isso significa que $\mathbf{\Gamma}(\mathcal{N}(\hat{\rho})^G) = \mathbf{\Gamma}(\mathcal{N}(\hat{\rho}^G)) = \mathbf{\Gamma}'$. Como o primeiro momento passa pelo mesmo tipo de evolução, $\mathcal{N}(\hat{\rho}^G) = \mathcal{N}(\hat{\rho})^G$ para qualquer $\hat{\rho} \in \mathcal{D}(\mathcal{H})$ e então $\Delta(\mathcal{N}, \hat{\rho}) = 0$ para $\hat{\rho}$ arbitrário. ■

O resultado do Lema 6.19 fornece uma condição suficiente para classificar um canal quântico em relação à sua não gaussianidade: se o funcional $\Delta(\mathcal{N}, \hat{\rho}) \neq 0$ para qualquer estado quântico $\hat{\rho}$, então $\mathcal{N}$ é nG. Se definirmos $\mathcal{F} = \{\mathcal{N} \in \mathcal{Q} : \Delta(\mathcal{N}, \hat{\rho}) \geq 0, \forall, \hat{\rho} \in \mathcal{D}(\mathcal{H})\}$, temos $\mathcal{G} \subset \mathcal{F}$ e é possível propor o seguinte.

Teorema 6.20. *Se $\mathcal{N} \in \mathcal{F}$ então $\delta_{vN}(\mathcal{N}(\hat{\rho})) \leq \delta_{vN}(\hat{\rho})$ para qualquer $\hat{\rho} \in \mathcal{D}(\mathcal{H})$.*

Demonstração. Seja $\hat{\rho}$ e $\mathcal{N}$ como no enunciado. Da contratividade de entropia relativa quântica para canais quânticos, temos que,

$$\delta_{vN}(\hat{\rho}) \overset{(a)}{=} S(\hat{\rho}||\hat{\rho}^G) \tag{6.56}$$

$$\overset{(b)}{\geq} S(\mathcal{N}(\hat{\rho})||\mathcal{N}(\hat{\rho}^G)) \tag{6.57}$$

$$\overset{(c)}{=} \mathrm{tr}[\mathcal{N}(\hat{\rho})(\log\mathcal{N}(\hat{\rho}) - \log\mathcal{N}(\hat{\rho}^G))] + \mathrm{tr}[(\mathcal{N}(\hat{\rho}) - \mathcal{N}(\hat{\rho})^G)\log\mathcal{N}(\hat{\rho})^G] \tag{6.58}$$

$$\overset{(d)}{=} S(\mathcal{N}(\hat{\rho})^G) - S(\mathcal{N}(\hat{\rho})) + \Delta(\mathcal{N},\hat{\rho}) \tag{6.59}$$

$$\overset{(e)}{=} S(\mathcal{N}(\hat{\rho})||\mathcal{N}(\hat{\rho})^G) + \Delta(\mathcal{N},\hat{\rho}) \tag{6.60}$$

$$\overset{(f)}{\geq} \delta_{vN}(\mathcal{N}(\hat{\rho})), \tag{6.61}$$

onde (a) vem da definição de δ_{vN}, (b) da monotonicidade da entropia relativa quântica [113], (c) tem-se que $\mathrm{tr}[(\hat{\sigma} - \hat{\sigma}^G)\log(\hat{\sigma}^G)] = 0$ para arbitrário $\hat{\sigma}$ [103], (d) usamos a definição no Lema 6.19, (e) de Definição 6.7 e (e) porque $\mathcal{N}$ e $\hat{\rho}$ foram escolhidos tal que $\Delta(\mathcal{N},\hat{\rho}) \geq 0$. ■

O resultado acima estende a propriedade da monotonicidade decrescente de δ_{vN} sob canais quânticos gaussianos para canais nG e também fornece uma interpretação da quantidade dada por $\Delta(\mathcal{N},\hat{\rho})$: se é não negativa para todo $\hat{\rho}$, $\mathcal{N}$ não aumenta o QRE-nG. Note que a diferença $S(\hat{\rho}||\hat{\rho}^G) - S(\mathcal{N}(\hat{\rho})||\mathcal{N}(\hat{\rho}^G))$ está relacionada a mapas de recuperação de estado (Petz recovery maps), os quais são mapas que podem recuperar o estado que sofreu alguma evolução física. Ressaltamos também que os mapas de recuperação podem ser estendidos para sistemas quânticos em dimensões infinitas [114]. No entanto, a especificação de $\mathcal{F}$ pode ter sido muito ampla ao exigir que $\Delta(\mathcal{N},\hat{\rho})$ seja não negativo para todos os estados quânticos do sistema, de modo que não é possível afirmar se $\mathcal{F} \setminus \mathcal{G} = \{\varnothing\}$ ou não. Um relaxamento na condição pode ser feito considerando apenas um conjunto específico de estados quânticos, que escolhemos como os estados relevantes para o contexto dos protocolos DM-CVQKD, e pode ser útil na descrição de um conjunto de canais quânticos não crescentes QRE-nG.

Seja $\mathcal{S}_{\bar{m}} = \left\{\hat{\sigma} \in \mathcal{D}(\mathcal{H}) : \hat{\sigma} = \sum_{x\in\mathcal{X}_n} p(x)\hat{\rho}^{th}(x,\bar{m})\right\}$ com X_n sendo uma variável aleatória simétrica discreta e $\hat{\rho}^{th}(x,\bar{m})$ o estado térmico deslocado com $\bar{m}$ fótons médios e o primeiro momento $\bar{\boldsymbol{x}} = 2\cdot(\mathrm{Re}\{x\},\mathrm{Im}\{x\})^T$. Constelações de estados coerentes são representadas pelo conjunto $\mathcal{S}_0$ e qualquer estado em $\mathcal{S}_{\bar{m}}$ tem uma matriz de covariância diagonal para qualquer valor de $\bar{m}$, o que significa que seu estado quântico gaussiano equivalente é um estado térmico com o número médio apropriado de fótons. Então, é possível definir um conjunto $\mathcal{F}_{\bar{m}} = \{\mathcal{N} \in \mathcal{Q} : \Delta(\mathcal{N},\hat{\rho}) \geq 0, \forall, \hat{\rho} \in \mathcal{S}_{\bar{m}}\}$ tal que o QRE-nG de qualquer estado quântico em $\mathcal{S}_{\bar{m}}$ não aumenta sob a ação de qualquer canal em $\mathcal{F}_{\bar{m}}$.

Além disso, temos que $\mathcal{G} \subset \mathcal{F} \subset \mathcal{F}_{\bar{m}}$ para qualquer $\bar{m}$. Os estados em $\mathcal{S}_{\bar{m}}$ são relevantes para a configuração do protocolo QKD porque representam a saída de misturas de estados por um canal gaussiano com ruído térmico $\bar{m}$.

Proposição 6.21. $\mathcal{F}_0 \setminus \mathcal{G} \neq \{\varnothing\}$.

Demonstração. Assuma o processo de difusão de fase. Foi desenvolvido que a QRE-nG de estados coerentes sob difusão de fase aumenta com o tempo e que para qualquer $\hat{\rho} \in \mathcal{S}_0$, $\bar{\boldsymbol{x}}(\hat{\rho}) = \bar{\boldsymbol{x}}(\mathcal{N}_\Delta(\hat{\rho}))$ e $\boldsymbol{\Gamma}(\hat{\rho}) = \boldsymbol{\Gamma}(\mathcal{N}_\Delta(\hat{\rho}))$, o que implica que $\hat{\rho}^G = \mathcal{N}_\Delta(\hat{\rho})^G$. Ou seja, o processo de difusão de fase não modifica o primeiro e segundo momentos estatísticos de misturas apropriadas de estados coerentes. Além disso, não tem efeito sobre os estados térmicos, ou seja, $\mathcal{N}_\Delta(\hat{\rho}^G) = \hat{\rho}^G$. Concluímos que $\mathcal{N}_\Delta(\hat{\rho}^G) = \mathcal{N}_\Delta(\hat{\rho})^G$ que resulta em $\Delta(\mathcal{N}_\Delta, \hat{\rho}) = 0$ para qualquer estado em $\mathcal{S}_0$ e então em $\mathcal{F}_0 \setminus \mathcal{G} \neq \{\varnothing\}$. ■

Conjecturamos que a Proposição 6.21 pode ser estendida para outros valores de $\bar{n}$ diferentes de zero, embora ainda não tenhamos provado isso. Na Figura 28, apresentamos a QRE-nG de constelações de estados coerentes que sofrem o processo de difusão de fase. A curva azul superior corresponde à medida QRE-nG para as constelações antes do processo ocorrer, e calculamos $\delta_{vN}(\mathcal{N}_\Delta(\hat{\rho}_{X_n}))$ para $\lambda = 0.15$ (curva vermelha) e $\lambda = \infty$ (curva verde), que têm o efeito de decoerência total na mistura de estados coerentes, destruindo os elementos fora da diagonal na matriz de densidade. Como esperado, a ação de $\mathcal{N}_\Delta$ não aumenta o QRE-nG da constelação uma vez que $\hat{\rho}_{X_n} \in \mathcal{S}_0$.

Além do fato de que o processo de difusão de fase preserva a propriedade de monotonicidade decrescente da QRE-nG quando restrito a um conjunto apropriado de estados quânticos, o fato de deixar a matriz de covariância invariante da constelação é uma implicação interessante para os protocolos DM-CVQKD. Defina por $\mathcal{T}$ o conjunto de canais quânticos que preservam o primeiro e segundo momentos de qualquer estado quântico em $\mathcal{S}_{\bar{n}}$ para qualquer valor de $\bar{n}$. Agora, pegue um canal gaussiano $\mathcal{N}_1$ com transmitância τ e ruído de excesso ξ e qualquer canal quântico $\mathcal{N}_2 \in \mathcal{T}$. Na etapa de estimação de parâmetros de um protocolo DM-CVQKD, Alice e Bob usam parte dos dados para estimar a transmitância do canal e o excesso de ruído para reconstruir a matriz de covariância do estado bipartido no protocolo emaranhado. Essa matriz de covariância é usada para calcular os limitantes da informação Holevo para a informação da espiã, e todo canal quântico compatível com os parâmetros estimados deve ser considerado.

A ideia aqui é que os canais quânticos considerados em uma análise de segurança DM-CVQKD podem ser divididos em dois canais, o gaussiano $\mathcal{N}_1$ produzindo os parâmetros observados e $\mathcal{N}_2$, que não modifica a matriz de covariância (e, portanto, não

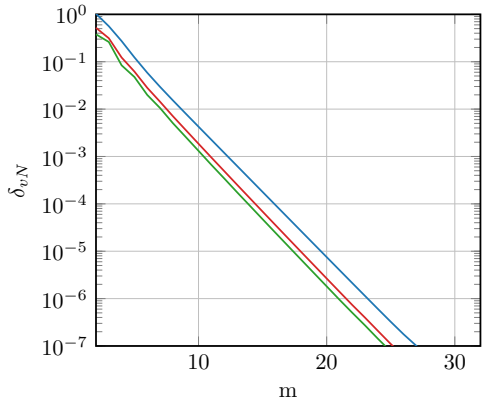


Figura 28 – Valores do QRE-nG para a constelação GQ-QAM sob um processo de difusão de fase com variação de modulação fixa $\bar{m} = 2.5$ e tamanho crescente da constelação. A linha superior (azul) corresponde à constelação nG anterior ao canal e na constelação em processo com os parâmetros $\gamma = 0.15$ e $\gamma = \infty$, respectivamente.

afeta a estimativa dos parâmetros), mas é responsável por interações não gaussianas que são responsáveis por "diminuir" a taxa de chave do protocolo para além do limite das iterações gaussianas.

6.2 Erro de Aproximação e Convergência da Purificação

Na Seção 6.1.3, a quantidade ε_G, a diferença (na taxa de chave secreta) entre o protocolo com modulação discreta e seu equivalente gaussiano, foi descrita como uma medida de não gaussianidade de um protocolo DM-CVQKD. Essa medida quantifica a quantidade de chave secreta perdida ao usar um modelo gaussiano para um protocolo com modulação não gaussiana. Na Equação (5.10), ε_G se refere à desigualdade da direita, e os resultados levam à conclusão de que $\varepsilon_G \to 0$ com o aumento da constelação se $X_n \Rightarrow X_G$, o que significa que o uso do limitante inferior calculado pelo estado gaussiano equivalente resulta em uma perda de chave gerada que pode ser considerada negligível se a constelação for grande o suficiente.

Contudo, a convergência de ε_G não fornece uma justificativa para os resultados apresentados no Capítulo 3, onde a lacuna de capacidade - a diferença entre a taxa de chave calculada para o protocolo com modulação discreta e o protocolo com modulação contínua gaussiana, que se refere à desigualdade da esquerda em (5.10) - se torna desprezível também com o aumento da cardinalidade da constelação. O Teorema 6.15, resultado central para a análise do comportamento de ε_G, assegura a convergência de $\hat{\rho}_{X_n}$ para uma mistura gaussiana de estados coerentes, mas não pode ser utilizado para analisar o comportamento do termo $Z^*(\tau, \xi)$, Equação (3.51).

Para apresentar uma justificativa formal para a aparente convergência (em taxa de chave secreta) da modulação discreta para a contínua gaussiana, é preciso justificar a convergência do estado bipartido (purificação) e também a convergência da matriz de covariância do estado gaussiano equivalente. O objetivo desta seção é explorar as consequências da convergência de operadores do Teorema 6.15 calculando cotas superiores para o erro de aproximação da convergência, bem como a convergência do estado bipartido que purifica a constelação. Para isso, utilizaremos a equivalência entre convergência fraca e convergência na norma de sequências de operadores lineares em $\mathcal{D}(\mathcal{H})$.

Teorema 6.22 (Convergência fraca implica convergência na norma [109])**.** *Seja $\{\hat{\sigma}_n\}$ uma sequência de operadores densidade em $\mathcal{D}(\mathcal{H})$ convergindo fracamente para $\hat{\sigma}$. Então $\{\hat{\sigma}_n\}$ converge na norma (do traço) para $\hat{\sigma}$.*

Uma consequência direta do Teorema 6.22 é que os operadores de densidade $\hat{\rho}_{X_n}$, conforme definidos na Seção 6.1.3 para representar constelações de estados coerentes, também convergem na norma do traço para a mistura gaussiana de estados coerentes, $\hat{\rho}_{X_G}$. É de interesse, no entanto, conhecer a velocidade de convergência da constelação. A próxima proposição apresenta uma cota superior para a distância entre $\hat{\rho}_{X_n}$ e $\hat{\rho}_{X_G}$ ao considerar uma redução da dimensão do subespaço relevante.

Proposição 6.23 (Erro de aproximação de sequências convergentes)**.** *Seja $\{\hat{\rho}_{X_n}\}$ e $\hat{\rho}_{X_G}$ como no Teorema 6.15 e $P_d = \sum_{k=0}^{d-1} |k\rangle\langle k|$. Então, $\|\hat{\rho}_{X_n} - \hat{\rho}_{X_G}\| = O((\frac{\bar{m}}{\bar{m}+1})^d)$.*

Demonstração. Defina os projetores $P_d = \sum_{k=0}^{d-1} |k\rangle\langle k|$ e $Q = I - P_d$ de modo que

$$\varepsilon = \operatorname{tr}(\hat{\rho}_{X_G} Q) = \sum_{k=d}^{\infty} \frac{\bar{m}^k}{(\bar{m}+1)^{k+1}} = \left(\frac{\bar{m}}{\bar{m}+1}\right)^d. \tag{6.62}$$

Então, para qualquer operador $A \in \mathcal{B}(\mathcal{H})$,

$$|\operatorname{tr}(\hat{\rho}_{X_G} Q A)| \leq \|\hat{\rho}_{X_G} Q\|_1 \|A\| = \varepsilon \|A\| \tag{6.63}$$

uma vez que $\operatorname{tr}(\rho_{X_G} P) = \|\rho_{X_G} P\|_1$ e $\operatorname{tr}(\rho_{X_G} Q) = \|\rho_{X_G} Q\|_1$. Seguindo o desenvolvimento de [115, Teorema 3] e usando a desigualdade (6.63), tem-se que $|\operatorname{tr}[(\hat{\rho}_n - \hat{\rho})A]| \leq 6 \cdot \varepsilon \|A\|$, de modo que

$$\|\hat{\rho}_n - \hat{\rho}\|_1 = \sup_{\|A\| \leq 1} |\operatorname{tr}[(\hat{\rho}_n - \hat{\rho})A]| = \sup_{\|A\| \leq 1} 6 \cdot \varepsilon \|A\| \leq 6\left(\frac{\bar{m}}{\bar{m}+1}\right)^d \tag{6.64}$$

■

O limite fornecido pela Proposição 6.23 está relacionado aos resultados desenvolvidos em [34], nos quais a segurança incondicional do protocolo com modulação gaussiana para

ataques arbitrários é reduzida para ataques coletivos por meio do uso de um teste de energia que realiza um truncamento do espaço de Fock. A próxima proposição relaciona a convergência da sequência de operadores à convergência do espectro de autovalores e autovetores. Para abordar essa questão, utilizaremos alguns resultados da teoria de perturbação de operadores lineares.

Perturbação de operadores lineares[10]

Considere um espaço de Banach[11] X e um operador linear $T \in \mathcal{B}(X)$. Um autovalor de T é definido como um número complexo λ tal que existe elemento não nulo u do domínio de T que satisfaz a identidade $Tu = \lambda u$, e u é um autovetor de T associado ao autovalor λ. Analogamente, λ é um autovalor de T se o núcleo N da transformação $T - \lambda$ é diferente de 0, sendo $\dim[N(T - \lambda)] = m$ a multiplicidade de λ. Assuma que T é fechado[12] em X. Então, $T - z$ é fechado para todo $z \in \mathbb{C}$ e se $T - z$ é inversível,

$$R(z) = R(z, T) = (T - z)^{-1} \in \mathcal{B}(X), \tag{6.65}$$

é chamado de resolvente de T e z pertence ao conjunto resolvente de T, definido como o complemento (em relação ao plano complexo) do espectro de T, isto é, $P(T) = \mathbb{C} \setminus \Lambda(T)$. O conjunto resolvente é um subconjunto de $\mathbb{C}$ para o qual, dado um elemento não nulo $v \in X$, existe uma solução para a equação

$$(T - z)u = v. \tag{6.66}$$

Considere o operador perturbado $T(x) = T + xT'$, $x \in \mathbb{C}$. $T(0)$ é chamado de operador não perturbado e é válido questionar o quanto o espectro de autovalores e os autovetores de $T(x)$ mudam conforme o operador é perturbado. Em geral, a perturbação será na mesma ordem de magnitude de $|x|$. Como, neste trabalho, será relevante analisar a perturbação dos autovalores e autovetores de acordo com a norma do operador de perturbação, $\|xT'\|$, utilizaremos a notação $A = xT'$ e denotaremos o operador perturbado por $T(x) = T + xT' = T + A = T_A$. Represente o resolvente do operador T perturbado por A por

$$R_A(z) = (T_A - z)^{-1}. \tag{6.67}$$

[10]Neste parágrafo destacado será feita uma breve introdução à teoria de perturbação de operadores lineares, sendo restrita apenas aos pontos necessários para a demonstração da Proposição 6.25. Para mais detalhes, vide o livro texto [116].

[11]Um espaço de Banach X é definido como um espaço vetorial normado e completo, em que completude está relacionada à existência de limite u de toda sequência de Cauchy $\{u_n\}$, $u_n, u \in X$. Um espaço de Hilbert será então um espaço de Banach cuja norma é induzida pelo produto interno.

[12]Um operador T é dito fechado se seu domínio for um conjunto fechado.

É possível representar o resolvente como uma série de potência em x (consequentemente em A), o que resulta em

$$R_A(z) = R(z)\sum_{p=0}^{\infty}[-AR(z)]^p = R(z) + R(z)\sum_{p=1}^{\infty}[-A\cdot R(z)]^p. \tag{6.68}$$

sendo $R(z) = R(z,0)$, é chama de segunda série de Neumann para o resolvente e denota os efeitos do operador A no conjunto resolvente, o qual é diretamente conectado ao espectro de autovalores. Do mesmo modo, é possível observar a perturbação nos autoprojetores de T. Seja λ um autovalor de T com multiplicidade m e Γ uma curva fechada em $P(T)$ contendo λ e mais nenhum outro autovalor de T. O operador definido por

$$P(x) = P_A = -\frac{1}{2\pi i}\int_{\Gamma} R_A(z)\,\mathrm{d}^2z = P_\lambda - \frac{1}{2\pi i}\int_{\Gamma} R(z)\sum_{p=1}^{\infty}[-AR(z)]^p\,\mathrm{d}^2z\,, \tag{6.69}$$

é um projetor que é igual à soma de todos os autoprojetores relacionados aos autovalores de T_A que estão dentro de Γ e $P_\lambda = P(0)$.

O seguinte teorema apresenta uma cota superior para a distância entre os autoespectros de operadores lineares, o que será útil na análise da convergência do autoespectro da sequência convergente de operadores de densidade [116, Capítulo V, Teorema 4.10].

Teorema 6.24 (Perturbação do autoespectro)**.** *Seja T um operador autoadjunto e $A \in \mathcal{B}(\mathcal{H})$ simétrico. Então $T_A = T + A$ é autoadjunto e* $\mathrm{dist}(\Lambda(S), \Lambda(T_A)) \leq \|A\|_1$*, sendo $\Lambda(\cdot)$ o espectro de autovalores do operador.*

Proposição 6.25. *Considere a convergência $\hat{\rho}_{X_n} \to \hat{\rho}_{X_G}$ e as decomposições espectrais $\hat{\rho}_{X_n} = \sum_{k=1}^{N}\lambda_{k,n}\,|\phi_{k,n}\rangle\langle\phi_{k,n}|$ e $\rho_{X_G} = \sum_{n=0}^{\infty}\frac{\bar{m}^n}{(\bar{m}+1)^{n+1}}\,|n\rangle\langle n| = \sum_{n=0}^{\infty}\lambda_n\,|n\rangle\langle n|$. Então,*

(i) Para todo $k \in \mathbb{N}$, $\lim_{n\to\infty}|\lambda_{k,n} - \lambda_k| = 0$,

(ii) Para todo $k \in \mathbb{N}$, $\lim_{n\to\infty}\||\phi_{k,n}\rangle\langle\phi_{k,n}| - |k\rangle\langle k|\|_1 = 0$

Demonstração. Tome $T_A = \hat{\rho}_{X_n}$ e $T = \hat{\rho}_{X_G}$ de modo que $A = \hat{\rho}_{X_n} - \hat{\rho}_{X_G}$. Para a primeira parte da proposição, o Teorema 6.24 resulta em $\mathrm{dist}(\Lambda(\hat{\rho}_{X_n}), \Lambda(\rho_{X_G})) \leq \|\hat{\rho}_{X_G} - \hat{\rho}_{X_n}\|$, que pode ser feito arbitrariamente pequeno com o aumento de n uma vez que a convergência fraca de operadores em $\mathcal{D}(\mathcal{H})$ coincide com a convergência na norma do traço. Para a segunda parte, tome um autovalor λ_k de T e uma curva fechada (suave) Γ_{λ_k} em $P(T_A)$ contendo λ_k e mais nenhum outro autovalor de T. Usando a expressão em (6.69),

$$P_A = -\frac{1}{2\pi i}\int_{\Gamma_{\lambda_k}}\left[R(z) + R(z)\sum_{p=1}^{\infty}[-A\cdot R(z)]^p\right]\mathrm{d}^2z\,, \tag{6.70}$$

$$= P_{\lambda_k} - \frac{1}{2\pi i}\int_{\Gamma_{\lambda_k}} R(z)\sum_{p=1}^{\infty}[-A\cdot R(z)]^p\,\mathrm{d}^2z\,, \tag{6.71}$$

sendo P_{λ_k} o projetor correspondente ao autovalor λ_k de T e o termo restante relativo à "perturbação" A. Desenvolvendo o somatório, temos que

$$\sum_{p=1}^{\infty}[-A\cdot R(z)]^p = -AR(z) + AR(z)AR(z) - AR(z)AR(z)AR(z) + \cdots \tag{6.72}$$

$$= A[-R(z) + R(z)AR(z) - R(z)AR(z)AR(z) + \cdots], \tag{6.73}$$

de modo que

$$P_A = P_{\lambda_k} - \frac{1}{2\pi i}\int_{\Gamma_{\lambda_k}} R(z)A[-R(z) + R(z)AR(z) - R(z)AR(z)AR(z) + \cdots]\,\mathrm{d}^2z \tag{6.74}$$

Então, a diferença entre os projetores será

$$\|P_{\lambda_k} - P_A\| = \frac{1}{2\pi}\left\|\int_{\Gamma_{\lambda_k}} R(z)A[-R(z) + R(z)AR(z)\cdots]\,\mathrm{d}^2z\right\| \tag{6.75}$$

$$\leq \frac{1}{2\pi}\int_{\Gamma_{\lambda_k}} \|R(z)A\|\|[-R(z) + R(z)AR(z)\cdots]\|\,\mathrm{d}^2z \tag{6.76}$$

$$\leq \frac{1}{2\pi}\int_{\Gamma_{\lambda_k}} \|R(z)\|\cdot\|A\|\cdot\|-R(z) + R(z)AR(z)\cdots\|\,\mathrm{d}^2z \tag{6.77}$$

$$= \frac{\|A\|}{2\pi}\int_{\Gamma_{\lambda_k}} \|R(z)\|\cdot\|-R(z) + R(z)AR(z)\cdots\|\,\mathrm{d}^2z \tag{6.78}$$

que pode ser feito arbitrariamente pequeno uma vez que $\|A\| = \|\hat{\rho}_{X_G} - \hat{\rho}_{X_n}\|$. ■

Um exemplo da convergência dos projetores é observado quando comparamos as decomposições espectrais dos operadores de densidade referentes às constelações dos protocolos BPSK [87], QPSK [48] e o protocolo com oito estados e modulação APSK [40]. Sem entrar nos detalhes das expressões das respectivas diagonalizações e purificações, as três constelações são representadas pelos seguintes operadores de densidade,

$$\hat{\rho}_{(2)} = \sum_{k=0}^{1}\lambda_{k,2}\,|\phi_{k,2}\rangle\langle\phi_{k,2}|\,, \qquad |\phi_{k,2}\rangle = \frac{e^{-\alpha^2/2}}{\sqrt{\lambda_{k,2}}}\sum_{l=0}^{\infty}(e^{\pi/4})^{k-1}\frac{(-i)^l\alpha^{2l+k}}{\sqrt{(2l+k)!}}\,|2l+k\rangle\,, \tag{6.79}$$

$$\hat{\rho}_{(4)} = \sum_{k=0}^{3}\lambda_{k,4}\,|\phi_{k,4}\rangle\langle\phi_{k,4}|\,, \qquad |\phi_{k,4}\rangle = \frac{e^{-\alpha^2/2}}{\sqrt{\lambda_{k,4}}}\sum_{l=0}^{\infty}\frac{(-1)^l\alpha^{4l+k}}{\sqrt{(4l+k)!}}\,|4l+k\rangle\,, \tag{6.80}$$

$$\hat{\rho}_{(8)} = \sum_{k=0}^{7}\lambda_{k,8}\,|\phi_{k,8}\rangle\langle\phi_{k,8}|\,, \qquad |\phi_{k,8}\rangle = \frac{e^{-\alpha^2/2}}{\sqrt{\lambda_{k,8}}}\sum_{l=0}^{\infty}\frac{\alpha^{8l+k}}{\sqrt{(8l+k)!}}\,|8l+k\rangle\,, \tag{6.81}$$

onde pode ser visto que, à medida que o tamanho da constelação aumenta, o projetor $|\phi_{0,n}\rangle$, por exemplo, passa de uma superposição dos estados da base de Fock com "múltiplos de 2" ($|0\rangle, |2\rangle, \ldots$) para uma superposição de estados "múltiplos de 8", em que a contribuição do estado $|0\rangle$ aumenta. Com o aumento da cardinalidade, a constelação se aproxima da distribuição gaussiana e a contribuição das bases diferentes de $|0\rangle$ se torna praticamente nula.

A convergência dos projetores permite observar a convergência em norma por outra perspectiva. Utilizando a seguinte identidade,

$$\begin{aligned}\|S_n - S\|_1 \leq & \|P(S_n - S)P\|_1 + \|(I-P)S_n(I-P)\|_1 + \|(I-P)S(I-P)\|_1 + \\ & 2\|PS(I-P)\|_1 + 2\|PS_n(I-P)\|_1, \end{aligned} \tag{6.82}$$

a qual é válida para qualquer projetor de dimensão finita [109, Lema 11.1], e usando o $P = \Pi$, o projetor descrito na Equação (3.39), é possível desenvolver a desigualdade (6.82) e obter

$$\|S_n - S\|_1 \leq 2[1 - \mathrm{tr}(\Pi S)] + \sqrt{\mathrm{tr}(\Pi S)}\sqrt{1 - \mathrm{tr}(\Pi S)} \tag{6.83}$$

$$= 2\varepsilon' + \sqrt{1-\varepsilon'}\sqrt{\varepsilon'} \tag{6.84}$$

$$\leq 2\varepsilon' + \sqrt{\varepsilon'}, \tag{6.85}$$

em que $\varepsilon' = 1 - \mathrm{tr}(\Pi S)$, $0 \leq \varepsilon' \leq 1$ e, como Π é um projetor no subespaço gerado pelos estados coerentes da constelação, temos que $\mathrm{tr}(\Pi S_n) = 1$ e $\mathrm{tr}((I - \Pi)S_n) = 0$. Desenvolvendo $\mathrm{tr}(\Pi S)$,

$$\mathrm{tr}(\Pi S) = \mathrm{tr}\left[\sum_k |\phi_k\rangle\langle\phi_k| \sum_{l=0}^{\infty} \frac{\bar{m}^l}{(\bar{m}+1)^{l+1}} |l\rangle\langle l|\right] \tag{6.86}$$

$$= \sum_{l=0}^{\infty} \frac{\bar{m}^l}{(\bar{m}+1)^{l+1}} \sum_k |\langle l|\phi_k\rangle|^2 \tag{6.87}$$

$$\to 1, \tag{6.88}$$

de modo que $\varepsilon' \to 0$ com o aumento da cardinalidade da constelação. Esse resultado funciona como uma espécie de recíproca para a Proposição 6.25, em que a convergência na norma implica a convergência dos projetores, e agora a convergência dos projetores implica a convergência na norma do traço. Agora, tendo explorado a convergência dos autovalores e autovetores como consequência da convergência fraca de operadores, é possível abordar a convergência do estado purificado.

Proposição 6.26. *Seja $X_G \sim \mathbb{CN}(0, \bar{m})$ e $\{X_n\}_{n\in\mathbb{N}}$ assim como no Teorema 6.15 e $|\Phi_{AB_n}\rangle = (\mathbb{1}_A \otimes \hat{\rho}_{X_n}^{\frac{1}{2}}) \sum_{n=0}^{\infty} |n\rangle|n\rangle$ uma purificação de $\hat{\rho}_{X_n}$. Então $\hat{\rho}_{AB_n} \to \hat{\rho}_{AB}$, sendo $\hat{\rho}_{AB_n} = |\Phi_{AB_n}\rangle\langle\Phi_{AB_n}|$ a purificação da constelação (Equação (3.34)) e $\hat{\rho}_{AB} = |\nu\rangle\langle\nu|$ o estado EPR com $\nu = 2\bar{m} + 1$.*

Demonstração.

$$\hat{\rho}_{AB_n} = |\Phi_{AB_n}\rangle\langle\Phi_{AB_n}| = \left(\sum_l |l\rangle \otimes \hat{\rho}_{X_n}^{\frac{1}{2}} |l\rangle\right)\left(\sum_m \langle m| \otimes \langle m| \hat{\rho}_{X_n}^{\frac{1}{2}}\right) \tag{6.89}$$

$$= \sum_{l,m} |l\rangle\langle m| \otimes \hat{\rho}_{X_n}^{\frac{1}{2}} |l\rangle\langle m| \hat{\rho}_{X_n}^{\frac{1}{2}} \tag{6.90}$$

$$= \sum_{l,m} |l\rangle\langle m| \otimes \sum_{j,k} \sqrt{\lambda_{j,n}\lambda_{k.n}} |\phi_{j,n}\rangle\langle\phi_{j,n}| |l\rangle\langle m| |\phi_{k,n}\rangle\langle\phi_{k,n}| \tag{6.91}$$

$$\overset{(n)}{\to} \sum_{l,m} |l\rangle\langle m| \otimes \sum_{j,k} \sqrt{\lambda_j\lambda_k} \langle j|l\rangle \langle m|k\rangle |j\rangle\langle k| \tag{6.92}$$

$$= \sum_{l,m} |l\rangle\langle m| \otimes |l\rangle\langle m| \cdot \frac{1}{\bar{m}+1}\left[\left(\frac{\bar{m}}{\bar{m}+1}\right)^{\frac{1}{2}}\right]^{l+m}, \tag{6.93}$$

em que a convergência dos autovalores e autovetores é conforme a Proposição 6.25. Fazendo $\bar{m} = \sinh^2(r)$ e $\lambda = \tanh(r)$, temos que $1/(\bar{m}+1) = 1 - \tanh^2(r) = 1 - \lambda^2$ e $\sqrt{\bar{m}/(\bar{m}+1)} = \sqrt{\tanh^2(r)} = \sqrt{\tanh^2(-r)} = \tanh(-r) = -\tanh(r) = -\lambda$. Assim,

$$\hat{\rho}_{AB_n} \to \sum_{l,m} |l\rangle\langle m| \otimes |l\rangle\langle m| \cdot (1-\lambda^2) \cdot (-\lambda)^{l+m} = \hat{\rho}_{AB}. \tag{6.94}$$

Alternativamente, tome $|\psi\rangle, |\gamma\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$ arbitrários de modo que, sem perda de generalidade, podem ser decompostos como $|\psi\rangle = |\psi\rangle_A |\psi\rangle_B$ e $|\gamma\rangle = |\gamma\rangle_A |\gamma\rangle_B$. Então

$$\langle\psi|\hat{\rho}_{AB_n}|\gamma\rangle = \langle\psi|_A \langle\psi|_B \left(\sum_{j,k=1}^{(n+1)^2} \sqrt{\lambda_j\lambda_k} |\phi_j\rangle |\phi_j\rangle \langle\phi_k|\phi_k\rangle\right) |\gamma\rangle_A |\gamma\rangle_B \tag{6.95}$$

$$= \sum_{j,k=1}^{(n+1)^2} \sqrt{\lambda_j\lambda_k}\, {}_A\langle\psi|\phi_j\rangle\, {}_B\langle\psi|\phi_j\rangle \langle\phi_k|\gamma\rangle_A \langle\phi_k|\gamma\rangle_B \tag{6.96}$$

$$\overset{n}{\to} \sum_{j,k=1}^{\infty} \frac{\bar{m}}{\bar{m}+1}\left[\left(\frac{\bar{m}}{\bar{m}+1}\right)^{\frac{1}{2}}\right]^{j+k} {}_A\langle\psi|j\rangle\, {}_B\langle\psi|j\rangle \langle k|\gamma\rangle_A \langle k|\gamma\rangle_B \tag{6.97}$$

$$= \langle\psi|\hat{\rho}_{AB}|\gamma\rangle, \tag{6.98}$$

de modo que $\hat{\rho}_{AB_n}$ converge fracamente para $\hat{\rho}_{AB}$ e, consequentemente, converge em norma. ■

Tendo tratado da convergência da purificação do estado bipartido que purifica a constelação, o próximo passo é lidar com a matriz de covariância, especificamente com o limitante inferior Z^* para a covariância entre quadraturas de modos diferentes. Como já discutido, a quantidade de informação da espiã é inversamente proporcional à magnitude de Z^*, e os resultados do Capítulo 3 que mostram a taxa de chave secreta de modulações

do tipo QAM próximas das taxas para a modulação contínua gaussiana indicam que Z^* se aproxima de Z.

Entre os termos relevantes, V_A e V_B dependem apenas da energia média do esquema de modulação, que é um parâmetro do protocolo e não depende do tipo específico de formato da constelação. Desse modo, a taxa de chave, sendo uma função da matriz de covariância, na qual esta difere apenas no termo da diagonal secundária (do ponto de vista de uma matriz em bloco), temos que, usando o produto interno de Hilbert-Schmidt para matrizes $\langle A, B\rangle = \mathrm{tr}(A^\dagger B)$ e a norma induzida, a distância $d_{HS}(\cdot,\cdot)$ entre as matrizes

$$\mathbf{\Gamma}(\hat{\rho}_{AB}) = \begin{pmatrix} V_A\boldsymbol{I} & Z\boldsymbol{\sigma}_z \\ Z\boldsymbol{\sigma}_z & V_B\boldsymbol{I} \end{pmatrix} \qquad \mathbf{\Gamma}(\hat{\rho}_{AB_n}) = \begin{pmatrix} V_A\boldsymbol{I} & Z_n^*\boldsymbol{\sigma}_z \\ Z_n^*\boldsymbol{\sigma}_z & V_B\boldsymbol{I} \end{pmatrix} \tag{6.99}$$

será

$$\begin{aligned}
d_{HS}(\mathbf{\Gamma}(\hat{\rho}_{AB}), \mathbf{\Gamma}(\hat{\rho}_{AB_n})) &= [\langle \mathbf{\Gamma}(\hat{\rho}_{AB}) - \mathbf{\Gamma}(\hat{\rho}_{AB_n}), \mathbf{\Gamma}(\hat{\rho}_{AB}) - \mathbf{\Gamma}(\hat{\rho}_{AB_n})\rangle]^{\frac{1}{2}} && (6.100)\\
&= \left[\mathrm{tr}(\mathbf{\Gamma}(\hat{\rho}_{AB}) - \mathbf{\Gamma}(\hat{\rho}_{AB_n}))^2\right]^{\frac{1}{2}}, && (6.101)\\
&= \left(\mathrm{tr}\left[\begin{pmatrix} \mathbf{0} & (Z - Z_n^*)\boldsymbol{I} \\ (Z - Z_n^*)\boldsymbol{I} & \mathbf{0} \end{pmatrix}^2\right]\right)^{\frac{1}{2}} && (6.102)\\
&= \sqrt{4(Z - Z^*)^2} && (6.103)\\
&= 2|Z - Z_n^*| && (6.104)\\
&= 2|2\sqrt{\tau}\sqrt{\bar{m}^2 + \bar{m}} - \sqrt{\tau}\,\langle \Phi_{AB_n}|\hat{a}\hat{b} + \hat{a}^\dagger\hat{b}^\dagger|\Phi_{AB_n}\rangle + \sqrt{2\tau\xi w}| && (6.105)\\
&= 2|2\sqrt{\tau}\sqrt{\bar{m}^2 + \bar{m}} - \sqrt{\tau}\,\mathrm{tr}[\hat{\rho}_{AB_n}(\hat{a}\hat{b} + \hat{a}^\dagger\hat{b}^\dagger)] + \sqrt{2\tau\xi w}| && (6.106)\\
&\to 0, && (6.107)
\end{aligned}$$

uma vez que w depende de $\hat{\rho}_{X_n}$ e, no limite $\lim_{n\to\infty}\hat{\rho}_{X_n} = \hat{\rho}_{X_G}$, $w \to 0$; analogamente, pela convergência do estado bipartido, $\mathrm{tr}[\hat{\rho}_{AB_n}(\hat{a}\hat{b} + \hat{a}^\dagger\hat{b}^\dagger)] \to 2\sqrt{\bar{m}^2 + \bar{m}}$.

6.2.1 Segurança Incondicional e Protocolos com Modulação Discreta

Os resultados até aqui apresentados foram desenvolvidos sob a hipótese de ataques coletivos gaussianos, os quais, conforme descrito nas Seções 2.2 e 5.1, podem representar o efeito da transmissão de estados quânticos por fibras ópticas, em que os parâmetros do canal são constantes e o sistema completo pode ser representado por um estado composto separável. No entanto, a classe de ataques arbitrários implica em uma forte restrição às capacidades da espiã. Isso ocorre porque, após L rodadas da etapa de comunicação quântica, o estado quântico compartilhado por Alice e Bob é representado pelo operador

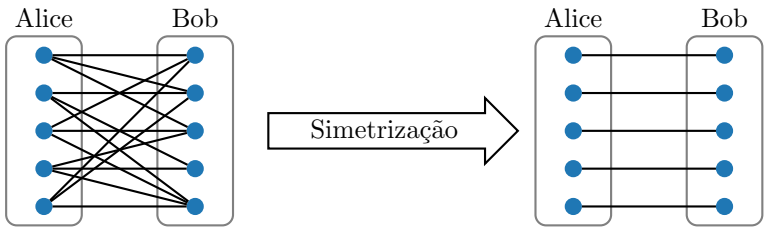


Figura 29 – Representação (informal) dos sistemas de Alice e Bob após a etapa de comunicação quântica. À esquerda, os diversos modos compartilhados apresentam correlações resultantes de uma evolução geral arbitrária realizada pela espiã, a qual dificulta a análise de segurança do protocolo. À direita, uma estrutura *iid* da etapa de comunicação que corresponde à espiã realizar ataques coletivos. As estratégias de prova de segurança universal do protocolo utilizam argumentos que se valem das simetrias dos protocolos para garantir a proximidade entre estruturas arbitrárias e *iid*. A simetria do protocolo pode ser reforçada por um processo ativo de simetrização e o protocolo seguro contra ataques coletivos será também seguro contra ataques arbitrários.

de densidade arbitrário[13] $\hat{\rho}_{AB}^{L} \in \mathcal{D}((\mathcal{H}_A \otimes \mathcal{H}_B)^{\otimes L})$. A segurança contra ataques coletivos é equivalente a assumir que $\hat{\rho}_{AB}^{L} = \hat{\sigma}_{AB}^{\otimes L}$, em que $\hat{\sigma} \in \mathcal{D}(\mathcal{H}_A \otimes \mathcal{H}_B)$ é um "estado protótipo", de modo que o sistema completo seja representado por uma estrutura *iid*.

Essa *redução* de um estado arbitrário para estados *iid* corresponde exatamente a uma redução da classe de ataques arbitrários para ataques coletivos, conforme ilustrado na Figura 29, que é conhecida como redução de de Finetti [117]. Em termos gerais, um ataque arbitrário realizado pela espiã pode ser modelado como uma operação unitária universal nos L estados compartilhados por Alice e Bob, de modo que correlações são impressas entre os diferentes subsistemas compartilhados. O ataque coletivo corresponde à preservação da estrutura *iid* do protocolo, e a redução consiste em mostrar a equivalência entre os dois tipos de ataques. Portanto, um protocolo seguro contra ataques coletivos também será seguro contra ataques arbitrários.

Um protocolo QKD, de forma formal para fins de definição da segurança incondicional, é representado por um mapa CPTP $\mathcal{E}$ que mapeia o conjunto de estados quânticos compartilhados por Alice e Bob (estados bipartidos emaranhados) na tripla (S_A, S_B, C), em que S_A e S_B são as chaves em posse de Alice e Bob[14], respectivamente, após a execução do protocolo, e C é a transcrição da comunicação clássica realizada. O protocolo ideal $\mathcal{F}$ é modelado pela concatenação de um mapa CPTP $\mathcal{S}$ com $\mathcal{E}$, levando a

[13] Aqui, o expoente funciona como um indicador da quantidade de sistemas bipartidos que $\hat{\rho}_{AB}$ representa, a fim de diferenciá-lo do estado bipartido $\hat{\rho}_{AB}$.

[14] Em provas de composibilidade, o fator ϵ_{cor} compõe o parâmetro de segurança geral do protocolo, limitando superiormente a probabilidade de o protocolo falhar na etapa de correção de erros e amplificação de privacidade, ou seja, $\Pr[S_A \neq S_B] \leq \epsilon_{cor}$. Portanto, é necessário considerar, na definição do protocolo, a possibilidade de as chaves geradas serem diferentes.

tripla (S_A, S_B, C) para a tripla (S, S, C), em que S é uma chave secreta perfeita (uniformemente distribuída e desconhecida por Eva) com o mesmo comprimento de S_A, utilizando a mesma comunicação clássica C, de modo que $\mathcal{F} = \mathcal{S} \circ \mathcal{E}$.

Definição 6.27 (Segurança do protocolo QKD)**.** *Seja $\mathcal{E}$ um mapa CPTP que representa o protoclo QKD e $\mathcal{F}$ o protocolo ideal correspondente. Então $\mathcal{E}$ é ϵ-seguro se*

$$\frac{1}{2}\|\mathcal{E} - \mathcal{F}\|_{\diamondsuit} \leq \epsilon. \tag{6.108}$$

em que $||\cdot||_{\diamondsuit}$ é a distância do diamante para canais quânticos (Definição B.27). O protocolo $\mathcal{E}$ será então seguro contra ataques arbitrários com parâmetro de segurança ε (seguro-ε) se a probabilidade de distingui-lo de $\mathcal{F}$ for menor que ε. Duas técnicas são empregadas para realizar a redução de ataques arbitrários para coletivos. A primeira consiste na aplicação dos teoremas quânticos de de Finetti, que limitam a distância do traço entre estados arbitrários e estados *iid* ou "quase *iid*". A segunda abordagem limita a distância do diamante entre protocolos considerando a atuação do protocolo em "estados de de Finetti", que são combinações convexas de estados *iid*.

Simetrização

As técnicas de *postselection* e de Finetti são utilizadas para protocolos (ou para estados multimodo) que apresentam algum tipo de simetria em sua estrutura. O objetivo é aproveitar possíveis invariâncias em relação a operações de um grupo simétrico para garantir a possibilidade de redução de ataques arbitrários para ataques coletivos, que podem ser "forçados" por meio de um processo ativo de simetrização. Por exemplo, para sistemas invariantes sob permutações, Alice e Bob podem escolher ignorar as correlações entre os N subsistemas compartilhados, considerando que $\hat{\rho}_{AB}^{L}$ tem a forma compatível com um ataque coletivo ou, de forma mais rigorosa, eles podem forçar a simetria aplicando uma permutação π implementada pelo operador $\hat{P}_{\pi}$, que é escolhida aleatoriamente do grupo de permutação $\mathcal{S}_n$, e depois "esquecendo" a informação sobre qual permutação foi realizada, levando ao estado simetrizado

$$\hat{\rho}_{AB}^{(s)} = \frac{1}{n!}\sum_{\pi \in \mathcal{S}_n} \hat{P}_{\pi}\hat{\rho}_{AB}^{L}\hat{P}_{\pi}^{\dagger}. \tag{6.109}$$

Na prática, a simetrização de $\hat{\rho}_{AB}^{L}$ é equivalente a Alice e Bob aplicarem uma permutação nos rótulos das chaves brutas que, em última análise, implica na simetria do protocolo: a operação de permutação comuta com os procedimentos de medição e pós-processamento clássico das chaves brutas. Portanto, o procedimento de simetrização consiste em mostrar que sempre é possível transformar $\hat{\rho}_{AB}^{L}$ no estado $\hat{\rho}_{AB}^{(s)}$ por meio de

permutações dos subsistemas, e que esse procedimento é equivalente a mostrar que o protocolo é suficientemente simétrico para que Alice e Bob possam assumir *a priori* que $\hat{\rho}_{AB}^{L}$ é simétrico *para a geração de chaves secretas*.

O ponto central do argumento é que Alice e Bob não utilizarem informações sobre a ordem dos elementos da chave bruta durante as etapas de medição e pós-processamento clássico é equivalente à aplicação de uma permutação e "esquecer" qual permutação foi realizada. Além da simetrização por permutação aleatória, rotações no espaço de fase também podem ser utilizadas para garantir a redução para ataques coletivos. Vale destacar que estados simétricos não necessariamente apresentam a estrutura *iid* resultante dos ataques coletivos. Portanto, o objetivo dos teoremas de Finetti e de *postselection* é mostrar a equivalência entre estados *iid* e estados simétricos.

Teoremas Quânticos de de Finetti

O teorema da representação global de de Finetti[15] aplicado a sistemas quânticos mostra que um estado simétrico se aproxima de um estado *iid* à medida que é aplicado o traço parcial em alguns subsistemas,

$$|| \operatorname{tr}_{n-k}(\hat{\rho}_{AB}) - \hat{\omega}|| \leq \epsilon', \tag{6.110}$$

onde $\hat{\omega} = \int \hat{\sigma}^{\otimes k} p(\sigma)\, \mathrm{d}\sigma$ é uma mistura de estados *iid* $\hat{\sigma}_{AB} \in \mathcal{D}(\mathcal{H}^{\otimes k})$, para alguma medida de probabilidade $p(\sigma)$ [75]. Assim, se um protocolo é seguro contra ataques coletivos, ele também será seguro contra ataques arbitrários desde que apresente as simetrias relevantes para o contexto, ou seja, invariância sob permutações nos subsistemas [76]. Para protocolos com variáveis discretas, o erro de aproximação é limitado superiormente por $\epsilon' = 2kd^2/n$, sendo $d = \dim(\mathcal{H})$, o que impossibilita o uso dessa técnica para a segurança do protocolo QKD, uma vez que o erro é proporcional a k/n, exigindo que o traço parcial seja aplicado na maioria dos subsistemas para obter uma aproximação suficientemente boa.

O teorema *exponencial* de de Finetti [76] propõe o relaxamento da condição *iid* do teorema inicial. Um estado $\hat{\rho}^{\otimes n}$ qualquer é dito (n, m)-*iid* com relação a algum protótipo $\hat{\sigma}$ se puder ser representado como a composição de um estado *iid* $\hat{\sigma}^{\otimes m} \in \mathcal{D}(\mathcal{H}^{\otimes m})$ e um estado qualquer $\hat{\rho}_{n-m} \in \mathcal{D}(\mathcal{H}^{\otimes(n-m)})$, exceto por uma permutação π nos subsistemas,

$$\hat{\rho}^{\otimes n} = \hat{P}_{\pi}(\hat{\sigma}^{\otimes m} \otimes \hat{\rho}_{n-m})\hat{P}_{\pi}^{\dagger}. \tag{6.111}$$

[15] No caso clássico, o teorema de Finetti afirma que sistemas compostos descritos por distribuições conjuntas de probabilidade invariantes sob permutações podem ser aproximados por uma mistura probabilística de variáveis aleatórias *iid*[117].

Portanto, o teorema exponencial de de Finetti garante que, em um sistema de N modos, qualquer subsistema de n modos pode ser aproximado por uma mistura de estados $(n, n-r)$-*iid* com protótipo $\hat{\sigma}$, em que $r \ll n$, de modo que o erro de aproximação seja $\epsilon = 3(N-n)^d e^{-r(N-n)/N}$. A interpretação operacional desse relaxamento é a ocorrência de algum evento de perturbação em r subsistemas de um estado *iid*, o qual, em um protocolo QKD, não afeta a segurança da chave.

Técnica de Postselecttion

Um caminho para alcançar a segurança incondicional em um protocolo QKD sem utilizar alguma versão do teorema de Finetti é por meio da técnica de *postselection* [118], que analisa a segurança de um protocolo QKD através do limite superior para a distância entre um protocolo real e um protocolo ideal, em que $\Delta = \mathcal{E} - \mathcal{F}$ é invariante sob permutações dos subsistemas. Seguindo o teorema de *postselection*, o protocolo $\mathcal{E}$ é ϵ-seguro contra ataques arbitrários se

$$\|\mathcal{E}-\mathcal{F}\|_{\diamondsuit} = \sup_{\hat{\rho}^L_{ABE}} \left\|(\mathcal{E}-\mathcal{F})\otimes \mathbb{1}(\hat{\rho}^L_{ABE})\right\| \leq (n+1)^{d^2-1}\|(\mathcal{E}-\mathcal{F})\otimes \mathbb{1}(\hat{\omega}_{ABE})\| = \epsilon'(n+1)^{d^2-1} \tag{6.112}$$

em que ϵ' é o parâmetro de segurança contra ataques coletivos (que pode ser feito arbitrariamente pequeno, $\epsilon' \leq 2^{-c\delta^2 n}$), $\epsilon = \epsilon'(n+1)^{d^2-1}$.

Perspectivas para Protocolos DM-CVQKD

As duas técnicas utilizadas para reduzir a classe de ataques arbitrários para ataques coletivos são eficazes no contexto de protocolos QKD com variáveis discretas, como o BB84, mas não são diretamente aplicáveis na análise de protocolos com variáveis contínuas devido à dimensão do espaço de Hilbert. Uma solução é utilizar um teste de energia antes da execução do protocolo em conjunto com um projetor em um subespaço de dimensão finita d. A ideia é que se os estados medidos por Bob apresentam uma energia média inferior a um parâmetro pré-estabelecido, a probabilidade do estado bipartido compartilhado por Alice e Bob "residir" em um subespaço de dimensão finita aumenta exponencialmente com d.

Em particular, a prova de segurança contra ataques arbitrários desenvolvida em [34] do protocolo[16] $\mathcal{E}_0$ utiliza um teste de energia $\mathcal{T}$ e a projeção $\mathcal{P}$ em um subespaço d-dimensional de modo que

$$\|\mathcal{E}-\mathcal{F}\|_{\diamondsuit} \leq \|\tilde{\mathcal{E}}-\tilde{\mathcal{F}}\|_{\diamondsuit} + 2\|(\mathbb{1}-\mathcal{P})\circ\mathcal{T}\|_{\diamondsuit}, \tag{6.113}$$

[16] O protocolo analisado utiliza modulação gaussiana combinado com detecção heteródina.

sendo $\mathcal{E} = \mathcal{E}_0 \circ \mathcal{T}$, $\mathcal{F} = \mathcal{S} \circ \mathcal{E}$, $\tilde{\mathcal{E}} = \mathcal{E}_0 \circ \mathcal{P} \circ \mathcal{T}$ e $\tilde{\mathcal{F}} = \mathcal{S} \circ \mathcal{E}_0$. Utilizando o mapa projetor em um subespaço de dimensão finita, foi possível utilizar os resultados do teorema de *Postselection* para limitar o primeiro termo do lado direito da desigualdade (6.113), enquanto o segundo termo foi limitado superiormente fixando o estado da otimização da distância do diamante por um estado produto, equivalente à hipótese de um ataque coletivo, de modo que

$$\|(\mathbb{1} - \mathcal{P}) \circ \mathcal{T}\|_{\diamondsuit} \leq \epsilon_{test} = O\left(\left(\frac{\bar{m}}{\bar{m}+1}\right)^{d}\right). \tag{6.114}$$

O termo ϵ_{test} denota exatamente a probabilidade do estado compartilhado por Alice e Bob passar no teste de energia $\mathcal{T}$ e estar fora do subespaço d-dimensional relevante para a análise de segurança, o que diminui exponencialmente com d e é proporcional à distância entre um estado térmico e uma mistura convergente de estados coerentes (Proposição 6.23). Portanto, é esperado que o fator de segurança incondicional para um protocolo com modulação discreta, em que a constelação converge em distribuição para uma curva gaussiana, seja proporcional à segurança desenvolvida em [34] para um protocolo com modulação contínua.

No entanto, ainda existem fatores de ordem operacional que podem tornar as provas de segurança incondicional desenvolvidas para protocolos gaussianos incompatíveis com protocolos de modulação não gaussiana, principalmente devido aos procedimentos de simetrização utilizados para garantir os argumentos de simetria necessários. Os teoremas de Finetti e de *postselection* assumem que o protocolo é invariante sob permutações, e em [34, 35, 36], as provas de segurança (e composabilidade) de protocolos com modulação gaussiana utilizam operações lineares passivas (divisores de feixe e deslocamentos de fase) antes da medição dos estados recebidos por Bob, a fim de aplicar rotações no espaço de fase para explorar a invariância do protocolo em relação a rotações. Como discutido na Seção 4.1, a arquitetura de um transmissor para constelações com formatação probabilística seria incompatível com permutações aleatórias dos subsistemas, o que impede que o protocolo apresente a propriedade necessária nas hipóteses da prova de segurança.

No caso das rotações no espaço de fase, um problema em potencial é que as rotações no espaço de fase resultam em rotações no vetor que representa os resultados das medições. A possibilidade de reverter o efeito do procedimento de simetrização pela aplicação da operação inversa R^{-1} não resolve o problema, uma vez que os protocolos DM-CVQKD devem usar uma arquitetura de detecção otimizada que esteja em sintonia com o formato da constelação. Portanto, em princípio, é ingênuo assumir que aplicar o procedimento de simetrização no estado multimodo e, em seguida, reverter o efeito aplicando uma rotação nos dados de medição mantém a performance do protocolo intacta. Para isso, é necessário

garantir que a operação que realiza rotações no espaço de fase comute com o sistema de detecção de pulsos coerentes e estimativa de símbolos da constelação, cuja descrição em termos de POVMs ainda não é conhecida até o momento [119]. Além disso, o procedimento de simetrização, que corresponde a uma rede de divisores de feixe e deslocamentos de fase, torna-se impraticável em cenários realistas com uma grande quantidade de estados transmitidos.

É importante ressaltar ainda que a hipótese utilizada em [120], de que para um protocolo com modulação não gaussiana em que a distância $\|\hat{\rho} - \hat{\sigma}\| \leq \epsilon_{\text{prep}}$ e o protocolo com modulação gaussiana possui segurança incondicional ϵ, o protocolo não gaussiano seria então $(\epsilon+\epsilon_{\text{prep}})$-seguro, onde ϵ_{prep} engloba um "erro de preparação" do estado térmico em uma modulação gaussiana, derivado em [121]. O problema dessa abordagem é que em [121], o erro de preparação refere-se à limitação do dispositivo de modulação em gerar valores truncados na preparação de estados coerentes e é calculado no cenário em que o protocolo em execução é com modulação gaussiana, de modo que Bob e Eva esperam observar um estado térmico. Portanto, o fator de segurança não se aplica diretamente ao caso de modulações discretas, em que não há erro de truncamento na modulação e Bob (e Eva) não esperam observar um estado térmico na saída do laboratório de Alice.

Convergência de Operadores e Erro de Aproximação

Neste capítulo, exploramos a convergência em distribuição de variáveis aleatórias para demonstrar a convergência da taxa de chave secreta de um protocolo com modulação discreta em direção ao limite superior dado pela modulação contínua gaussiana. Utilizamos como argumento principal que uma sequência de medidas de probabilidade que converge em distribuição induz uma sequência de operadores de densidade convergindo fracamente. Isso nos permitiu provar que o erro de aproximação do limite inferior da taxa de chave secreta, calculado a partir do estado gaussiano equivalente, decresce exponencialmente com o tamanho da constelação, uma vez que a medida de não gaussianidade da constelação diminui com o aumento da constelação. Também mostramos a existência de canais não gaussianos para os quais a medida de não gaussianidade é decrescente.

Explorando os resultados de convergência dos operadores de densidade, utilizamos a equivalência entre convergência fraca e convergência na norma (no conjunto dos operadores de densidade) para obter cotas superiores para o erro de aproximação da convergência, as quais estão relacionadas aos parâmetros de segurança incondicional do protocolo. Os resultados obtidos para sistemas de um modo foram generalizados para estados bipartidos, em particular, a convergência das purificações das constelações. Isso

nos permitiu demonstrar a convergência do termo de covariância das respectivas matrizes de covariância, o que justifica a convergência das taxas de chave secreta com o aumento da cardinalidade da constelação.

Parte IV

Conclusão

Capítulo 7

Considerações Finais

Os protocolos de distribuição quântica de chave secreta compreendem a primeira aplicação robusta da teoria da informação quântica, fornecendo segurança incondicional a sistemas de criptografia simétrica com base em argumentos da teoria da informação. Neste trabalho de tese, foram abordados os aspectos de desempenho e segurança de protocolos QKD em sistemas de variáveis contínuas e com modulação não gaussiana discreta. A apresentação da estrutura básica dos protocolos CVQKD foi apresentada no Capítulo 2 enquanto a fundamentação teórica em mecânica quânticas e teoria da informação clássica e quânticas está contidas nos Apêndices.

Em específico, no Capítulo 2 foram descritas as etapas de um protocolo de distribuição de chaves, bem como os três grupos que englobam as principais estratégias de espionagem que são consideradas na análise de segurança, ataques individuais, coletivo e arbitrários, e o modelo de ataque de clonagem por máquina de emaranhamento. Também foi apresentada a analise de segurança (para ataques coletivos) dos dois protocolos CVQKD que serviram de referência na análise de desempenho para a modulação discreta, o GG02 e UD-CVQKD.

O Capítulo 3 tratou de apresentar os protocolos com modulação discreta. Inicialmente, foi realizada uma discussão sobre o papel das modulações discretas no contexto das comunicações clássicas e como a capacidade do canal gaussiano pode ser aproximada pelo uso de esquemas de modulação discreta com sinalização não equiprovável. Em seguida, o desempenho dos protocolos QKD utilizando constelações de estados coerentes foi analisado e comparado com protocolos que utilizam modulação contínua gaussiana, observando sob quais condições a diferença em taxa de chave secreta desaparece. A análise realizada levou em consideração constelações com estados modulados em uma e duas dimensões e os resultados apontam que as constelações que alcançam a capacidade do canal aditivo gaussiano (comunicações clássicas) aproximam

as taxas de chave secreta esperadas para protocolos QKD com modulação gaussiana, desde que as constelações sejam grande o suficiente.

No Capítulo 4 foi abordado como a utilização de constelações com formatação probabilística e a arquitetura do transmissor que realiza esse tipo de formatação pode comprometer a invariância do protocolo a permutações dos estados compartilhados, a qual é fundamental am algumas formas de provar a segurança incondicional do protocolo. A dependência da sequência específica de símbolos enviados se dá pelo algoritmo que faz o mapeamento de sequências binárias em símbolos não equiprováveis (CCDM) que gera correlações entre os símbolos de saída. Como possível solução, foi apresentado um protocolo de reconciliação que converte sequências de símbolos não equiprováveis em sequências de *bits iid* e preserva o protocolo invariante a permutações.

O Capítulo 5 inicia a discussão sobre como as análises de segurança utilizam o teorema da extremalidade gaussiana para obter limitantes inferiores para a taxa de chave secreta do protocolo, o qual pode resultar na subestimação da capacidade do protocolo gerar chaves. Como alternativa, foi proposta a análise do ataque da espiã pela decomposição do ataque de emaranhamento utilizando a decomposição de Bloch-Messiah da máquina de clonagem por emaranhamento, o qual é o modelo padrão para canais quânticos gaussianos.

O Capítulo 6 foi dedicado ao papel da convergência de medidas de probabilidade, utilizando resultados da teoria da informação clássica para desenvolver propriedades relevantes para os protocolos DM-CVQKD. Inicialmente, a diferença de taxa de chave secreta entre um protocolo DM-CVQKD e seu limitante inferior utilizando o estado gaussiano equivalente foi definida como uma medida de não gaussianidade do protocolo, a qual foi mostrada ser equivalente à soma da medida de não gaussianidade do operador de densidade e a lacuna de capacidade informacional clássica da constelação. Também foi mostrado que misturas de estados coerentes induzidas por sequências de variáveis aleatórias que convergem (em distribuição) para a distribuição gaussiana convergem fracamente para um estado térmico. Aplicando o resultado da convergência de operadores de densidade à medida de não gaussianidade do protocolo foi possível mostrar que a quantidade de taxa de chave secreta que é perdida por conta do limitante inferior que utiliza o estado gaussiano equivalente ao protocolo se torna insignificante com o aumento do tamanho da constelação. Também foi apresentado um exemplo de canal não gaussiano que preserva a monotonicidade da medida de não gaussianidade de estados quânticos.

Ainda explorando a convergência de operadores de densidade, foram apresentados limitantes superiores para o erro de aproximação na distância do traço. Mostrando que

a convergência fraca de operadores implica na convergência do espectro de autovalores e dos autovetores (autoestados), foi mostrado como a convergência em um modo implica na convergência do estado bipartido da respectiva purificação. Dessa maneira, foi possível relacionar a convergência das constelações com a convergência do limitante inferior da taxa de chave secreta para os valores do limitante superior do protocolo com modulação gaussiana contínua. Os limitantes de aproximação e argumentos de convergência foram utilizados para discutir como as provas de segurança incondicional desenvolvidas para protocolos CVQKD com modulação gaussiana podem ser adaptadas para protocolos DM-CVQKD e quais desafios são impostos.

7.1 Trabalhos Futuros

Os protocolos QKD que usam modulação discreta de sistemas de variáveis contínuas possibilita o uso dos sistemas de comunicações ópticas no estado da arte: sistemas de modulação e detecção por processamento digital de sinais especializados para modulações do tipo QAM, bem como códigos corretores de erro que, combinados com arquiteturas de formatação de constelação, permitem a transmissão de informação à capacidade clássica do canal óptico. Contudo, a análise de segurança para os protocolos com modulação discreta ainda esta em seus dias iniciais se comparada aos protocolos com modulação contínua gaussiana. Alguns dos pontos que ainda estão em aberto, do ponto de vista teórico e prático, são os seguintes:

- **Adaptação da arquitetura PCS/PAS para sistemas DM-CVQKD**
  Para compatibilidade com provas de segurança incondicional contra ataques arbitrários, o protocolo QKD deve apresentar simetrias que permitam estabelecer a equivalência entre ataques arbitrários e ataques coletivos, como invariância a rotações no espaço de fase ou permutações dos subsistemas. A estrutura do sistema de transmissão que realiza o mapeamento de sequências de *bits iid* em símbolos de uma constelação com formatação probabilística deve ser invariante à operações do grupo de permutações.

- **Segurança incondicional de protocolos DM-CVQKD**
  Considerar os efeitos da não gaussianidade da constelação de estados coerentes nas provas de segurança de protocolos com modulações discretas, assim como o erro de aproximação em relação ao estado com modulação gaussiana contínua. Os principais argumentos utilizados na redução para ataques coletivos (de Finetti e *Postselection*) são baseados na probabilidade de distinguir entre o estado final do sistema e um cenário ideal. Logo, para utilizar argumentos semelhantes, os

parâmetros de segurança devem ser adaptados para o caso em que o estado que representa o esquema de modulação não é um estado térmico.

- **Implementação e compatibilidade com sistemas usuais**
  Dada a compatibilidade dos protocolos em variáveis contínuas com dispositivos usuais de comunicações ópticas, a implementação dos protocolos em laboratórios permitirá caracterizar a eficiência de modulação e detecção característicos, bem como observar novas fontes de ruído que devem ser levadas em consideração. Inclusive, a investigação dos efeitos de copropagação e compartilhamento da infraestrutura com sistemas de transmissão clássica de informação.

Referências Bibliográficas

1 CERF, N. J.; IPE, A.; ROTTENBERG, X. Cloning of Continuous Quantum Variables. *Phys. Rev. Lett.*, American Physical Society ({APS}), v. 85, n. 8, p. 1754–1757, 2000. Citado na página 24.

2 NIELSEN, M.; CHUANG, I. L. *Quantum Computation and Quantum Information: 10th Anniversary Edition*. [S.l.]: Cambridge University Press, 2010. ISSN 00029505. ISBN 1-107-00217-6. Citado nas páginas 24 e 195.

3 HEISENBERG, W. Über den anschaulichen Inhalt der quantentheoretischen Kinematik und Mechanik. *Zeitschrift für Physik*, v. 43, n. 3-4, p. 172–198, mar. 1927. ISSN 1434-6001, 1434-601X. Citado na página 24.

4 COLES, P. J. et al. Entropic uncertainty relations and their applications. *Reviews of Modern Physics*, v. 89, n. 1, 2017. ISSN 15390756. Citado nas páginas 24 e 187.

5 LO, H.-K.; CHAU, H. F. Unconditional Security of Quantum Key Distribution over Arbitrarily Long Distances. *Science*, American Association for the Advancement of Science ({AAAS}), v. 283, n. 5410, p. 2050–2056, mar. 1999. Citado na página 24.

6 SHOR, P. W.; PRESKILL, J. Simple Proof of Security of the {BB}84 Quantum Key Distribution Protocol. *Phys. Rev. Lett.*, American Physical Society ({APS}), v. 85, n. 2, p. 441–444, jul. 2000. Citado na página 24.

7 MAYERS, D. Unconditional security in quantum cryptography. *Journal of the {ACM}*, Association for Computing Machinery ({ACM}), v. 48, n. 3, p. 351–406, 2001. Citado na página 24.

8 LEVERRIER, A.; GRANGIER, P. Unconditional security proof of long-distance continuous-variable quantum key distribution with discrete modulation. *Phys. Rev. Lett.*, v. 102, n. 18, 2009. ISSN 00319007. Citado nas páginas 24, 28, 91, 92, 93 e 104.

9 BENNETT, C. H.; BRASSARD, G. Quantum cryptography: Public key distribution and coin tossing. *Theoretical Computer Science*, Elsevier {BV}, v. 560, p. 7–11, 2014. Citado nas páginas 24 e 47.

10 EKERT, A. K. Quantum cryptography based on Bell's theorem. *Phys. Rev. Lett.*, American Physical Society, v. 67, n. 6, p. 661–663, 1991. Citado na página 24.

11 BENNETT, C. H. Quantum cryptography using any two nonorthogonal states. *Phys. Rev. Lett.*, American Physical Society ({APS}), v. 68, n. 21, p. 3121–3124, 1992. Citado na página 24.

12 SCARANI, V. et al. Quantum Cryptography Protocols Robust against Photon Number Splitting Attacks for Weak Laser Pulse Implementations. *Phys. Rev. Lett.*, American Physical Society, v. 92, n. 5, p. 57901, 2004. Citado na página 24.

13 GROSSHANS, F.; GRANGIER, P. Continuous Variable Quantum Cryptography Using Coherent States. *Phys. Rev. Lett.*, American Physical Society, v. 88, n. 5, p. 57902, jan. 2002. Citado nas páginas 24, 27, 40 e 82.

14 GROSSHANS, F. et al. Quantum key distribution using gaussian-modulated coherent states. *Nature*, Macmillian Magazines Ltd., v. 421, p. 238, 2003. Citado nas páginas 24, 27, 40 e 42.

15 WEEDBROOK, C. et al. Quantum cryptography without switching. *Phys. Rev. Lett.*, 2004. ISSN 00319007. Citado nas páginas 24, 40 e 82.

16 DIAMANTI, E. et al. Practical challenges in quantum key distribution. *npj Quantum Information*, v. 2, n. 1, p. 16025, nov. 2016. ISSN 2056-6387. Citado na página 24.

17 PIRANDOLA, S. et al. Advances in Quantum Cryptography. *arXiv:1906.01645 [math-ph, physics:physics, physics:quant-ph]*, jun. 2019. <http://arxiv.org/abs/1906.01645>. Citado na página 24.

18 ASSCHE, G. V.; CARDINAL, J.; CERF, N. J. Reconciliation of a quantum-distributed Gaussian key. *IEEE TIT*, v. 50, n. 2, p. 394–400, 2004. ISSN 0018-9448. Citado nas páginas 25, 36 e 76.

19 NGUYEN, K.-C.; ASSCHE, G. V.; CERF, N. J. Side-Information Coding with Turbo Codes and its Application to Quantum Key Distribution. In: *International Symposium on Information Theory and Its Applications*. Parma, Italy, October: [s.n.], 2004. Citado nas páginas 25 e 41.

20 BLOCH, M. et al. LDPC-based Gaussian key reconciliation. In: *2006 IEEE Information Theory Workshop*. Punta del Este, Uruguay: IEEE, 2006. p. 116–120. ISBN 978-1-4244-0035-5. Citado nas páginas 25 e 78.

21 BAI, Z.; YANG, S.; LI, Y. High-efficiency reconciliation for continuous variable quantum key distribution. *Japanese Journal of Applied Physics*, Japan Society of Applied Physics, v. 56, n. 4, p. 44401, mar. 2017. Citado nas páginas 25 e 41.

22 ARAÚJO, L.; ASSIS, F.; ALBERT, B. Novo protocolo de reconciliação de chaves secretas geradas quanticamente utilizando códigos LDPC no sentido Slepian-Wolf. In: *Anais de XXXVI Simpósio Brasileiro de Telecomunicações e Processamento de Sinais*. [S.l.]: Sociedade Brasileira de Telecomunicações, 2018. Citado nas páginas 25, 36, 78 e 81.

23 WOLF, M. M.; GIEDKE, G.; CIRAC, J. I. Extremality of Gaussian Quantum States. *Phys. Rev. Lett.*, American Physical Society, v. 96, n. 8, p. 080502, mar. 2006. Citado nas páginas 25, 91, 93 e 195.

24 García-Patrón, R.; CERF, N. J. Unconditional optimality of Gaussian attacks against continuous-variable quantum key distribution. *Physical Review Letters*, v. 97, n. 19, p. 1–4, 2006. ISSN 00319007. Citado nas páginas 25 e 91.

25 NAVASCUÉS, M.; GROSSHANS, F.; ACÍN, A. Optimality of Gaussian attacks in continuous-variable quantum cryptography. *Physical Review Letters*, v. 97, n. 19, p. 2–5, 2006. ISSN 00319007. Citado na página 25.

26 WU, Y.; VERDÚ, S. The impact of constellation cardinality on gaussian channel capacity. *2010 48th Annual Allerton Conference on Communication, Control, and Computing, Allerton 2010*, IEEE, p. 620–628, 2010. Citado nas páginas 25, 50, 51, 53, 54, 58, 59 e 116.

27 PILORI, D. *Advanced Digital Signal Processing Techniques for High-Speed Optical Communications Links*. Tese (Doutorado), 2019. Citado nas páginas 25, 50, 55 e 75.

28 YANKOVN, M. P. et al. Constellation Shaping for WDM Systems Using 256QAM/1024QAM with Probabilistic Optimization. *Journal of Lightwave Technology*, v. 34, n. 22, p. 5146–5156, 2016. ISSN 07338724. Citado na página 25.

29 DIAS, M. A.; de Assis, F. M. The impact of constellation cardinality on discrete unidimensional CVQKD protocols. *Quantum Information Processing*, v. 20, n. 9, p. 284, set. 2021. ISSN 1570-0755, 1573-1332. Citado nas páginas 25 e 55.

30 DENYS, A.; BROWN, P.; LEVERRIER, A. Explicit asymptotic secret key rate of continuous-variable quantum key distribution with an arbitrary modulation. *Quantum*, v. 5, p. 540, set. 2021. ISSN 2521-327X. Citado nas páginas 25, 28, 48, 66, 69, 70 e 71.

31 Wikipedia contributors. *Composability — Wikipedia, the Free Encyclopedia*. 2021. <https://en.wikipedia.org/w/index.php?title=Composability&oldid=1030547806>. Citado na página 26.

32 RENNER, R.; KÖNIG, R. Universally Composable Privacy Amplification Against Quantum Adversaries. In: HUTCHISON, D. et al. (Ed.). *Theory of Cryptography*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2005. v. 3378, p. 407–425. ISBN 978-3-540-24573-5 978-3-540-30576-7. Citado nas páginas 26 e 36.

33 RENNER, R. *Security of Quantum Key Distribuction*. [S.l.], 2008. v. 9, n. 1, 1–127 p. Citado nas páginas 26 e 36.

34 LEVERRIER, A. et al. Security of continuous-variable quantum key distribution against general attacks. *Physical Review Letters*, v. 110, n. 3, p. 030502, jan. 2013. ISSN 0031-9007, 1079-7114. Citado nas páginas 26, 28, 68, 131, 141 e 142.

35 LEVERRIER, A. Composable security proof for continuous-variable quantum key distribution with coherent states. *Phys. Rev. Lett.*, v. 114, n. 7, 2015. ISSN 10797114. Citado nas páginas 26, 28 e 142.

36 LEVERRIER, A. Security of Continuous-Variable Quantum Key Distribution via a Gaussian de Finetti Reduction. *Phys. Rev. Lett.*, v. 118, n. 20, 2017. ISSN 10797114. Citado nas páginas 26, 28 e 142.

37 NASCIMENTO, E. J.; de Assis, F. M. Improving Continuous-Variable Quantum Key Distribution with Shannon-Kotel'nikov Maps. In: *2016 IEEE Globecom Workshops (GC Wkshps)*. Washington, DC, USA: IEEE, 2016. p. 1–6. ISBN 978-1-5090-2482-7. Citado na página 27.

38 SILBERHORN, Ch. et al. Continuous Variable Quantum Cryptography: Beating the 3 dB Loss Limit. *Physical Review Letters*, v. 89, n. 16, p. 167901, set. 2002. ISSN 0031-9007, 1079-7114. Citado na página 27.

39 ZHAO, Y. B. et al. Asymptotic security of binary modulated continuous-variable quantum key distribution under collective attacks. *Phys. Rev. A*, v. 79, n. 1, p. 1–14, 2009. ISSN 10502947. Citado nas páginas 27 e 28.

40 DJORDJEVIC, I. B. Optimized-Eight-State CV-QKD Protocol Outperforming Gaussian Modulation Based Protocols. *IEEE Photonics Journal*, v. 11, n. 4, p. 1–10, ago. 2019. ISSN 1943-0655, 1943-0647. Citado nas páginas 27, 28 e 134.

41 KAUR, E.; GUHA, S.; WILDE, M. M. Asymptotic security of discrete-modulation protocols for continuous-variable quantum key distribution. *Physical Review A*, v. 103, n. 1, p. 012412, jan. 2021. ISSN 2469-9926, 2469-9934. Citado nas páginas 27 e 28.

42 RENNER, R.; CIRAC, J. I. De Finetti representation theorem for infinite-dimensional quantum systems and applications to quantum cryptography. *Phys. Rev. Lett.*, v. 102, n. 11, p. 1–4, 2009. ISSN 00319007. Citado nas páginas 28 e 76.

43 LEVERRIER, A. A symmetrization technique for continuous-variable quantum key distribution. *Physical Review A*, v. 85, n. 2, p. 022339, fev. 2012. ISSN 1050-2947, 1094-1622. Citado na página 28.

44 SYCH, D.; LEUCHS, G. Coherent state quantum key distribution with multi letter phase-shift keying. *New Journal of Physics*, v. 12, n. 5, p. 053019, maio 2010. ISSN 1367-2630. Citado na página 28.

45 LEVERRIER, A.; GRANGIER, P. Continuous-variable quantum-key-distribution protocols with a non-Gaussian modulation. *Phys. Rev. A*, v. 83, n. 4, abr. 2011. ISSN 1050-2947. Citado nas páginas 28 e 93.

46 BRÁDLER, K.; WEEDBROOK, C. Security proof of continuous-variable quantum key distribution using three coherent states. *Phys. Rev. A*, v. 97, n. 2, p. 1–16, 2018. ISSN 24699934. Citado na página 28.

47 PAPANASTASIOU, P. et al. Quantum key distribution with phase-encoded coherent states: Asymptotic security analysis in thermal-loss channels. *Physical Review A*, v. 98, n. 1, p. 012340, jul. 2018. ISSN 2469-9926, 2469-9934. Citado nas páginas 28 e 95.

48 GHORAI, S. et al. Asymptotic Security of Continuous-Variable Quantum Key Distribution with a Discrete Modulation. *Physical Review X*, v. 9, n. 2, p. 021059, jun. 2019. ISSN 2160-3308. Citado nas páginas 28, 66, 76, 93 e 134.

49 LIN, J.; UPADHYAYA, T.; LÜTKENHAUS, N. Asymptotic Security Analysis of Discrete-Modulated Continuous-Variable Quantum Key Distribution. *Physical Review X*, v. 9, n. 4, p. 041064, dez. 2019. ISSN 2160-3308. Citado nas páginas 28 e 76.

50 ZHAO, W. et al. Unidimensional continuous-variable quantum key distribution with discrete modulation. *Physics Letters A*, v. 384, n. 2, p. 126061, jan. 2020. ISSN 03759601. Citado nas páginas 28 e 93.

51 GHALAII, M. et al. Discrete-Modulation Continuous-Variable Quantum Key Distribution Enhanced by Quantum Scissors. *IEEE Journal on Selected Areas in Communications*, v. 38, n. 3, p. 506–516, mar. 2020. ISSN 0733-8716, 1558-0008. Citado na página 28.

52 PAPANASTASIOU, P.; PIRANDOLA, S. Continuous-variable quantum cryptography with discrete alphabets: Composable security under collective Gaussian attacks. *Physical Review Research*, v. 3, n. 1, p. 013047, jan. 2021. ISSN 2643-1564. Citado na página 28.

53 KANITSCHAR, F. et al. *Finite-Size Security for Discrete-Modulated Continuous-Variable Quantum Key Distribution Protocols*. [S.l.]: arXiv, 2023. <http://arxiv.org/abs/2301.08686>. Citado na página 28.

54 SHANNON, C. E. Analogue of the Vernam System for Continuous Time. *SeriesBell Laboratories Memorandum*, IEEE, 1943. Citado na página 33.

55 LEVERRIER, A. *Theoretical Study of Continuous-Variable Quantum Key Distribution*. Tese (Doutorado) — Telecom ParisTech, 2010. Citado nas páginas 34 e 76.

56 CERF, N. J.; LEUCHS, G.; POLZIK, E. S. *Quantum Information with Continuous Variables of Atoms and Light*. [S.l.]: Icp, 2007. ISBN 978-1-86094-816-9. Citado nas páginas 37, 48 e 91.

57 SERAFINI, A. *Quantum Continuous Variables: A Primer of Theoretical Methods*. Boca Raton: CRC Press, Taylor & Francis Group, CRC Press is an imprint of the Taylor & Francis Group, an informa business, 2017. ISBN 978-1-4822-4634-6. Citado na página 37.

58 PIRANDOLA, S.; BRAUNSTEIN, S. L.; LLOYD, S. Characterization of Collective Gaussian Attacks and Security of Coherent-State Quantum Cryptography. *Physical Review Letters*, v. 101, n. 20, p. 200504, nov. 2008. ISSN 0031-9007, 1079-7114. Citado nas páginas 37 e 91.

59 LAUDENBACH, F. et al. Continuous-Variable Quantum Key Distribution with Gaussian Modulation-The Theory of Practical Implementations. *Advanced Quantum Technologies*, v. 1, n. 1, p. 1800011, 2018. ISSN 25119044. Citado nas páginas 37, 41, 47, 58, 82, 92 e 166.

60 GROSSHANS, F. CollectiveAttacks and Unconditional Security in Continuous Variable Quantum KeyDistribution. *Physical Review Letters*, v. 94, n. 2, p. 020504, jan. 2005. ISSN 0031-9007, 1079-7114. Citado na página 40.

61 LIVERIS, A.; Zixiang Xiong; GEORGHIADES, C. Compression of binary sources with side information at the decoder using LDPC codes. *IEEE Communications Letters*, v. 6, n. 10, p. 440–442, out. 2002. ISSN 1089-7798. Citado na página 41.

62 JOUGUET, P.; ELKOUSS, D.; Kunz-Jacques, S. High-bit-rate continuous-variable quantum key distribution. *Phys. Rev. A*, American Physical Society, v. 90, n. 4, p. 42329, 2014. Citado nas páginas 41 e 86.

63 USENKO, V. C.; GROSSHANS, F. Unidimensional continuous-variable quantum key distribution. *Physical Review A*, v. 92, n. 6, p. 062337, dez. 2015. ISSN 1050-2947, 1094-1622. Citado nas páginas 44 e 45.

64 WEEDBROOK, C. et al. Gaussian quantum information. *Rev. Mod. Phys.*, American Physical Society, v. 84, n. 2, p. 621–669, 2012. Citado nas páginas 47, 101 e 164.

65 COVER, J. A. T. T. M. *Elements of Information Theory*. [S.l.]: Wiley John + Sons, 2006. ISBN 0-471-24195-4. Citado nas páginas 48 e 79.

66 SCHWARTE, H. Approaching capacity of a continuous channel by discrete input distributions. *IEEE Transactions on Information Theory*, v. 42, n. 2, p. 671–675, mar. 1996. ISSN 00189448. Citado nas páginas 51, 52 e 53.

67 GRAY, R. M. *Entropy and Information Theory*. Boston, MA: Springer US, 2011. ISBN 978-1-4419-7969-8 978-1-4419-7970-4. Citado na página 52.

68 BILLINGSLEY, P. *Convergence of Probability Measures*. 2nd ed. ed. New York: Wiley, 1999. (Wiley Series in Probability and Statistics. Probability and Statistics Section). ISBN 978-0-471-19745-4. Citado nas páginas 53 e 121.

69 UNGERBOECK, G. Channel coding with multilevel/phase signals. *IEEE Transactions on Information Theory*, v. 28, n. 1, p. 55–67, jan. 1982. ISSN 0018-9448. Citado na página 53.

70 Feng-Wen Sun; van Tilborg, H. Approaching capacity by equiprobable signaling on the Gaussian channel. *IEEE Transactions on Information Theory*, v. 39, n. 5, p. 1714–1716, Sept./1993. ISSN 00189448. Citado na página 53.

71 SHANNON, C. E. A Mathematical Theory of Communication. *Bell System Technical Journal*, 1948. ISSN 15387305. Citado nas páginas 59 e 185.

72 DIAS, M. A.; ASSIS, F. M. de. Amplitude-Phase Modulated CVQKD Protocol. In: *Anais Do XXXIX Simpósio Brasileiro de Telecomunicações e Processamento de Sinais*. [S.l.]: Sociedade Brasileira de Telecomunicações, 2021. Citado na página 64.

73 CHO, J.; WINZER, P. J. Probabilistic Constellation Shaping for Optical Fiber Communications. *Journal of Lightwave Technology*, v. 37, n. 6, p. 1590–1607, mar. 2019. ISSN 0733-8724, 1558-2213. Citado na página 75.

74 SCHULTE, P.; BOCHERER, G. Constant Composition Distribution Matching. *IEEE Transactions on Information Theory*, v. 62, n. 1, p. 430–434, jan. 2016. ISSN 0018-9448, 1557-9654. Citado na página 75.

75 CHRISTANDL, M. et al. One-and-a-Half Quantum de Finetti Theorems. *Communications in Mathematical Physics*, v. 273, n. 2, p. 473–498, jun. 2007. ISSN 0010-3616, 1432-0916. Citado nas páginas 76 e 140.

76 RENNER, R. Symmetry implies independence. *Nature*, v. 3, n. September, p. 645–649, 2007. Citado nas páginas 76 e 140.

77 LEVERRIER, A. et al. Multidimensional reconciliation for a continuous-variable quantum key distribution. *Phys. Rev. A*, American Physical Society, v. 77, n. 4, p. 42325, 2008. Citado na página 76.

78 DIAS, M. A.; de Assis, F. M. *Distributional Transform Based Information Reconciliation*. [S.l.]: arXiv, 2023. <http://arxiv.org/abs/2204.08891>. Citado na página 77.

79 MILICEVIC, M. et al. Quasi-cyclic multi-edge LDPC codes for long-distance quantum cryptography. *npj Quantum Information*, v. 4, n. 1, p. 21, dez. 2018. ISSN 2056-6387. Citado na página 78.

80 MANI, H. et al. Multiedge-type low-density parity-check codes for continuous-variable quantum key distribution. *Physical Review A*, v. 103, n. 6, p. 062419, jun. 2021. ISSN 2469-9926, 2469-9934. Citado na página 78.

81 LODEWYCK, J. et al. Quantum key distribution over 25 km with an all-fiber continuous-variable system. *Phys. Rev. A*, v. 76, n. 4, 2007. ISSN 10941622. Citado na página 78.

82 DURANTE, F.; SEMPI, C. *Principles of Copula Theory*. Hoboken: CRC Press, 2016. <http://site.ebrary.com/id/11074681>. ISBN 978-1-4398-8442-3 978-1-4398-8444-7. Citado na página 78.

83 NHA, H.; CARMICHAEL, H. J. Distinguishing two single-mode Gaussian states by homodyne detection: An information-theoretic approach. *Physical Review A*, v. 71, n. 3, p. 032336, mar. 2005. ISSN 1050-2947, 1094-1622. Citado na página 82.

84 STEEG, G. V. *Gregversteeg/NPEET: Non-parametric Entropy Estimation Toolbox*. 2016. <https://github.com/gregversteeg/NPEET>. Citado na página 83.

85 KRASKOV, A.; STÖGBAUER, H.; GRASSBERGER, P. Estimating mutual information. *Physical Review E*, v. 69, n. 6, p. 066138, jun. 2004. ISSN 1539-3755, 1550-2376. Citado na página 83.

86 ASSCHE, G. V. *Quantum Cryptography and Secret-Key Distillation*. [S.l.]: CAMBRIDGE UNIV PR, 2006. ISBN 0-521-86485-2. Citado na página 85.

87 LEVERRIER, A.; GRANGIER, P. Continuous-variable Quantum Key Distribution protocols with a discrete modulation. *ArXiv*, fev. 2010. Citado nas páginas 94, 95, 105 e 134.

88 DIAS, M. A.; ASSIS, F. M. Evaluating the Eavesdropper Entropy via Bloch-Messiah Decomposition. In: *2021 IEEE Conference on Communications and Network Security (CNS)*. Tempe, AZ, USA: IEEE, 2021. p. 1–6. ISBN 978-1-66544-496-5. Citado na página 96.

89 BRAUNSTEIN, S. L. Squeezing as an irreducible resource. *Physical Review A*, v. 71, n. 5, p. 055801, maio 2005. ISSN 1050-2947, 1094-1622. Citado nas páginas 99 e 100.

90 CARIOLARO, G.; PIEROBON, G. Bloch-Messiah reduction of Gaussian unitaries by Takagi factorization. *PHYSICAL REVIEW A*, p. 7, 2016. Citado na página 100.

91 CARIOLARO, G.; PIEROBON, G. Reexamination of Bloch-Messiah reduction. *Physical Review A*, v. 93, n. 6, p. 062115, jun. 2016. ISSN 2469-9926, 2469-9934. Citado na página 100.

92 HORN, R. A.; JOHNSON, C. R. *Matrix Analysis*. 2nd ed. ed. Cambridge ; New York: Cambridge University Press, 2012. ISBN 978-0-521-83940-2. Citado na página 100.

93 CHITAMBAR, E.; GOUR, G. Quantum resource theories. *Reviews of Modern Physics*, v. 91, n. 2, p. 025001, abr. 2019. ISSN 0034-6861, 1539-0756. Citado nas páginas 110 e 111.

94 CHIRIBELLA, G.; D'ARIANO, G. M.; PERINOTTI, P. Transforming quantum operations: Quantum supermaps. *EPL (Europhysics Letters)*, v. 83, n. 3, p. 30004, ago. 2008. ISSN 0295-5075, 1286-4854. Citado na página 111.

95 FIURÁŠEK, J. Gaussian Transformations and Distillation of Entangled Gaussian States. *Physical Review Letters*, v. 89, n. 13, p. 137904, set. 2002. ISSN 0031-9007, 1079-7114. Citado na página 114.

96 GIEDKE, G.; CIRAC, J. I. Characterization of Gaussian operations and distillation of Gaussian states. *Physical Review A*, v. 66, n. 3, p. 032316, set. 2002. ISSN 1050-2947, 1094-1622. Citado na página 114.

97 NISET, J.; FIURÁŠEK, J.; CERF, N. J. No-Go Theorem for Gaussian Quantum Error Correction. *Physical Review Letters*, v. 102, n. 12, p. 120501, mar. 2009. ISSN 0031-9007, 1079-7114. Citado na página 114.

98 RALPH, T. C. et al. Quantum computation with optical coherent states. *Physical Review A*, v. 68, n. 4, p. 042319, out. 2003. ISSN 1050-2947, 1094-1622. Citado na página 114.

99 TAKAGI, R.; ZHUANG, Q. Convex resource theory of non-Gaussianity. *Physical Review A*, v. 97, n. 6, p. 062337, jun. 2018. ISSN 2469-9926, 2469-9934. Citado nas páginas 114 e 115.

100 GENONI, M. G.; PARIS, M. G. A.; BANASZEK, K. Measure of the non-Gaussian character of a quantum state. *Physical Review A*, v. 76, n. 4, p. 042327, out. 2007. ISSN 1050-2947, 1094-1622. Citado na página 114.

101 BAEK, K.; NHA, H. Non-Gaussianity and entropy-bounded uncertainty relations: Application to detection of non-Gaussian entangled states. *Physical Review A*, v. 98, n. 4, p. 042314, out. 2018. ISSN 2469-9926, 2469-9934. Citado na página 114.

102 GENONI, M. G.; PARIS, M. G. A.; BANASZEK, K. Quantifying the non-Gaussian character of a quantum state by quantum relative entropy. *Physical Review A*, v. 78, n. 6, p. 060303, dez. 2008. ISSN 1050-2947, 1094-1622. Citado na página 115.

103 HOLEVO, A. S.; SOHMA, M.; HIROTA, O. Capacity of quantum Gaussian channels. *Physical Review A*, v. 59, n. 3, p. 1820–1828, mar. 1999. ISSN 1050-2947, 1094-1622. Citado nas páginas 115, 128 e 195.

104 MARIAN, P.; MARIAN, T. A. Relative entropy is an exact measure of non-Gaussianity. *Physical Review A*, v. 88, n. 1, p. 012322, jul. 2013. ISSN 1050-2947, 1094-1622. Citado na página 115.

105 IVAN, J. S.; KUMAR, M. S.; SIMON, R. A measure of non-Gaussianity for quantum states. *Quantum Information Processing*, v. 11, n. 3, p. 853–872, jun. 2012. ISSN 1570-0755, 1573-1332. Citado na página 115.

106 ALBARELLI, F. et al. Resource theory of quantum non-Gaussianity and Wigner negativity. *Physical Review A*, v. 98, n. 5, p. 052350, nov. 2018. ISSN 2469-9926, 2469-9934. Citado na página 115.

107 ZHUANG, Q.; SHOR, P. W.; SHAPIRO, J. H. Resource theory of non-Gaussian operations. *Physical Review A*, v. 97, n. 5, p. 052317, maio 2018. ISSN 2469-9926, 2469-9934. Citado na página 115.

108 DIAS, M. A.; de Assis, F. M. *Converging State Distributions for Discrete Modulated CVQKD Protocols*. [S.l.]: arXiv, 2023. <http://arxiv.org/abs/2305.06484>. Citado na página 116.

109 HOLEVO, A. S. *Quantum Systems, Channels, Information: A Mathematical Introduction*. 2nd edition. ed. Berlin ; Boston: De Gruyter, 2019. (Texts and Monographs in Theoretical Physics). ISBN 978-3-11-064224-7. Citado nas páginas 120, 131 e 135.

110 LIU, Y.-x. et al. Kraus representation of a damped harmonic oscillator and its application. *Physical Review A*, v. 70, n. 4, p. 042308, out. 2004. ISSN 1050-2947, 1094-1622. Citado na página 124.

111 GENONI, M. G.; PARIS, M. G. A. Quantifying non-Gaussianity for quantum information. *Physical Review A*, v. 82, n. 5, p. 052341, nov. 2010. ISSN 1050-2947, 1094-1622. Citado na página 124.

112 MEMARZADEH, L.; MANCINI, S. Minimum output entropy of a non-Gaussian quantum channel. *Physical Review A*, v. 94, n. 2, p. 022341, ago. 2016. ISSN 2469-9926, 2469-9934. Citado na página 124.

113 WILDE, M. M. *Quantum Information Theory*. 2. ed. [S.l.]: Cambridge University Press, 2017. ISBN 978-1-107-17616-4. Citado nas páginas 128 e 190.

114 JUNGE, M. et al. Universal Recovery Maps and Approximate Sufficiency of Quantum Relative Entropy. *Annales Henri Poincaré*, v. 19, n. 10, p. 2955–2978, out. 2018. ISSN 1424-0637, 1424-0661. Citado na página 128.

115 WEHRL, A. Three theorems about entropy and convergence of density matrices. *Reports on Mathematical Physics*, v. 10, n. 2, p. 159–163, out. 1976. ISSN 00344877. Citado na página 131.

116 KATŌ, T. *Perturbation Theory for Linear Operators*. Berlin: Springer, 1995. (Classics in Mathematics). ISBN 978-3-540-58661-6. Citado nas páginas 132 e 133.

117 CAVES, C. M.; FUCHS, C. A.; SCHACK, R. Unknown quantum states: The quantum de Finetti representation. *Journal of Mathematical Physics*, American Institute of Physics, v. 43, n. 9, p. 4537–4559, set. 2002. ISSN 0022-2488. Citado nas páginas 138 e 140.

118 CHRISTANDL, M.; KÖNIG, R.; RENNER, R. Postselection Technique for Quantum Channels with Applications to Quantum Cryptography. *Physical Review Letters*, v. 102, n. 2, p. 020504, jan. 2009. ISSN 0031-9007, 1079-7114. Citado na página 141.

119 CHEN, Z. et al. Continuous-mode quantum key distribution with digital signal processing. *npj Quantum Information*, v. 9, n. 1, p. 28, mar. 2023. ISSN 2056-6387. Citado na página 143.

120 ROUMESTAN, F. et al. Demonstration of probabilistic constellation shaping for continuous variable quantum key distribution. In: *2021 Optical Fiber Communications Conference and Exhibition (OFC)*. [S.l.: s.n.], 2021. p. 1–3. Citado na página 143.

121 JOUGUET, P. et al. Analysis of imperfections in practical continuous-variable quantum key distribution. *Phys. Rev. A*, v. 86, p. 32309, 2012. Citado na página 143.

122 MA, X.; RHODES, W. Multimode squeeze operators and squeezed states. *Physical Review A*, v. 41, n. 9, p. 4625–4631, maio 1990. ISSN 1050-2947, 1094-1622. Citado na página 168.

123 BARNETT, S. M.; RADMORE, P. M. *Methods in Theoretical Quantum Optics*. Oxford : New York: Clarendon Press ; Oxford University Press, 1997. (Oxford Series in Optical and Imaging Sciences, 15). ISBN 978-0-19-856362-4. Citado na página 169.

124 JEONG, K.; LIM, Y. Purification of Gaussian maximally mixed states. *Physics Letters A*, v. 380, n. 43, p. 3607–3611, out. 2016. ISSN 03759601. Citado na página 169.

125 SHAPIRO, J. *6.453 Quantum Optical Communication*. [S.l.]: Massachusetts Institute of Technology: MIT OpenCourseWare, 2016. Citado na página 173.

126 LEONHARDT, U. *Measuring the Quantum State of Light*. New York: Cambridge University Press, 1997. (Cambridge Studies in Modern Optics, 22). ISBN 978-0-521-49730-5 978-0-521-02352-8. Citado na página 181.

127 JOZSA, R.; SCHLIENZ, J. Distinguishability of states and von Neumann entropy. *Physical Review A*, v. 62, n. 1, p. 012301, jun. 2000. ISSN 1050-2947, 1094-1622. Citado na página 188.

128 HUGHSTON, L. P.; JOZSA, R.; WOOTTERS, W. K. A complete classification of quantum ensembles having a given density matrix. *Physics Letters A*, v. 183, n. 1, p. 14–18, nov. 1993. ISSN 03759601. Citado na página 188.

129 WATROUS, J. *The Theory of Quantum Information*. Cambridge, United Kingdom: Cambridge University Press, 2018. ISBN 978-1-107-18056-7. Citado na página 196.

130 HELSTROM, C. W. *Quantum Detection and Estimation Theory*. New York: Academic Press, 1976. <http://www.sciencedirect.com/science/publication?issn=00765392&volume=123>. ISBN 978-0-08-095632-9. Citado na página 198.

Apêndice A

Mecânica Quântica e Sistemas de Variáveis Contínuas

A.1 Postulados da Mecânica Quântica

Postulado A.1 (Espaço de estados)**.** *Para qualquer sistema físico isolado existe um espaço vetorial complexo com produto interno (um espaço de Hilbert)* $\mathcal{H}$ *chamado de* espaço de estados *do sistema. O sistema é completamente descrito por um vetor de estados que é unitário no espaço de estados.*

Um sistema físico de grande interesse é o *qubit*, definido em um espaço de Hilbert $\mathcal{H} = \mathbb{C}$, sendo o sistema da mecânica quântica mais simples possível. Utilizando a notação de Dirac e sendo $|0\rangle$ e $|1\rangle$ uma base ortonormal para o espaço de estados (conhecida como base computacional), um estado qualquer deste espaço pode ser escrito como

$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle\,, \tag{A.1}$$

onde $\alpha,\ \beta \in \mathbb{C}$ e $|\alpha|^2 + |\beta|^2 = 1$. O estado representado pela equação A.1 se encontra em superposição (combinação linear de uma base ortonormal). O conjugado hermitiano (transposto conjugado) de $|\psi\rangle$ é representado por $\langle\psi|$ e o produto interno entre vetores é representado por $\langle\psi_1|\psi_2\rangle$.

Uma representação conveniente de estados quânticos é a por operadores de densidade que são utilizados quando o estado de um sistema não é completamente conhecido. O operador de densidade ρ é definido como uma combinação dos possíveis estados quânticos $|\psi_1\rangle\,, |\psi_2\rangle\,, \cdots\,, |\psi_N\rangle$ associados às probabilidades $p_1, p_2, \cdots, p_N$ $(\sum_i p_i = 1)$ do sistema estar no i-ésimo estado, de modo que

$$\hat{\rho} = \sum_{i=1}^{N} p_i\,|\psi_i\rangle\langle\psi_i|\,. \tag{A.2}$$

Quando o estado do sistema é puro, $\hat{\rho} = |\psi\rangle\langle\psi|$. O estado quântico pode ainda ser descrito como uma mistura de operadores de densidade, sendo um "mistura de misturas" $\hat{\rho} = \sum_i p_i \hat{\rho}_i$. Aqui, definimos o grau de mistura de um estado quântico $\hat{\rho}$ indicado pela quantidade $\mu(\hat{\rho})$

$$\mu(\hat{\rho}) = \mathrm{tr}(\hat{\rho}^2), \tag{A.3}$$

e um estado é dito puro s.s.s. $\mu(\hat{\rho}) = 1$. Para estados de sistemas com dimensão finita, $\dim(\mathcal{H}) = d < \inf$, $\frac{1}{d} \leq \mu(\hat{\rho}) \leq 1$ sendo os extremos superiores e inferiores indicando estados puros e maximamente misturados, respectivamente. Em sistemas de dimensão infinita, e.g., de variáveis contínuas, $0 \leq \mu(\hat{\rho}) \leq 1$.

Postulado A.2 (Evolução do sistema quântico)**.** *A evolução de um sistema quântico* fechado *é descrita por um operador unitário de transformação. Ou seja, um estado $|\psi\rangle$ no tempo t_1 evolui para o estado $|\psi'\rangle$ no tempo t_2 através do operador unitário $\hat{U}$, de modo que*

$$|\psi'\rangle = \hat{U}\,|\psi\rangle\,. \tag{A.4}$$

Alguns operadores têm utilização recorrente no estudo da informação de sistemas quânticos uma vez que apresentam comportamentos de portas quânticas análogas ao modelo clássico de computação. As *matrizes de Pauli* são representações de operações como a porta quântica NOT (matriz X) e a matriz Z a inversão de fase, com as seguintes representações matriciais na base computacional

$$\boldsymbol{X} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \boldsymbol{Y} = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \boldsymbol{Z} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad \boldsymbol{I} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}. \tag{A.5}$$

Postulado A.3 (Medição)**.** *Medidas quânticas são descritas por uma coleção de operadores de medição $\hat{M}_m$ que agem no espaço de estados do sistema a ser medido, onde o índice m se refere a uma possível saída do experimento.*

Para um sistema quântico que se encontra no estado $|\psi\rangle$ imediatamente antes da medição, a probabilidade de que seja obtido o resultado m é dada pela expressão

$$p(m) = \langle\psi|\,\hat{M}_m^\dagger \hat{M}_m\,|\psi\rangle \tag{A.6}$$

e o sistema após a medida colapsa para o estado

$$|\psi'\rangle = \frac{\hat{M}_m\,|\psi\rangle}{\sqrt{\langle\psi|\,\hat{M}_m^\dagger \hat{M}_m\,|\psi\rangle}}. \tag{A.7}$$

Os operadores de medição precisam satisfazer a relação de completude,

$$\sum_m \hat{M}_m^\dagger \hat{M}_m = I. \tag{A.8}$$

O tipo de medição descrita pelo Postulado A.3 é de certa forma generalista e alguns casos especiais de medição de sistemas quânticos podem ser derivados, os quais encontram aplicações importantes no processamento da informação, sendo as medições projetivas e POVM's (*Positive Operator-Valued Measure*).

Definição A.4 (Medição projetiva)**.** *Uma medição projetiva é descrita por um observável $\hat{M}$, que é um operador hermitiano no espaço de estados do sistema sendo observado, o qual tem uma decomposição espectral*

$$\hat{M} = \sum_m m\hat{P}_m, \tag{A.9}$$

em que $\hat{P}_m$ é o projetor no autoespaço de $\hat{M}$ com autovalor m.

A formulação da medição projetiva impõe uma condição forte sobre os operadores que podem descrever a medição do sistema, a hermiticidade de $\hat{M}$, o qual é chamado de observável.

Observáveis

Um observável é um operador do sistema e corresponde a uma grandeza mensurável, uma quantidade física acessível, como energia, posição, momento, etc.. Um observável $\hat{O}$ está associado com sua representação pela decomposição espectral

$$\hat{O} = \sum_n o_n \left|o_n\right\rangle\!\left\langle o_n\right|, \tag{A.10}$$

em que $\{o_n\}$ e $\{|o_n\rangle\}$ são seus autovalores e autovetores, respectivamente. Medir o observável $\hat{O}$, ou seja, medir a grandeza física associada ao operador $\hat{O}$, resulta em um valor real observado como saída do procedimento de medição, o qual será um dos elementos do conjunto de autovalores $\{o_n\}$. Pressupondo que o sistema está no estado $|\psi\rangle$ no instante imediatamente anterior à medição, a probabilidade de obter o valor medido o_n será

$$p(o_n|\,|\psi\rangle) = |\langle o_n|\psi\rangle|^2 = \mathrm{tr}(\hat{O}\,|\psi\rangle), \tag{A.11}$$

em que a última igualdade é a lei de Born.

A probabilidade de detecção e a evolução do estado após a medição seguem os mesmos parâmetros especificados pelo Postulado A.3 nas Equações (A.6) e (A.7), com a simplificação de que os projetores contêm as propriedades $\hat{P}_m^2 = \hat{P}_m$ e $\hat{P}_m\hat{P}_n = \delta_{mn}\hat{P}_m$. Logo, o estado é projetado no autoespaço do observável associado ao autovalor resultante da medição, e uma característica curiosa é a repetibilidade: dado que o procedimento de

medição de um estado teve resultado m, repetir a medição resulta na mesma saída e não mudará o estado.

Definição A.5 (POVM)**.** *Seja $\{\hat{M}_m\}$ um conjunto de operadores que descrevem uma medição. Um POVM é descrito pelo conjunto de operadores $\{\hat{E}_m\}$, sendo $\hat{E}_m = \hat{M}_m^\dagger \hat{M}_m$ e chamados de elementos do POVM.*

Em linhas gerais, medições descritas por POVM são aquelas para as quais o experimentalista não está preocupado com a evolução do estado após a medição, ou até mesmo para os casos em que o estado é destruído pelo dispositivo de detecção.

Postulado A.6 (Sistemas compostos)**.** *O espaço de estados de um sistema quântico composto é representado pelo produto tensorial do espaço de estados de cada componente físico do sistema. Em outras palavras, para n sistemas onde o i-ésimo sistema é preparado no estado $|\psi\rangle_i$, o sistema composto total é $|\psi_1\rangle \otimes |\psi_2\rangle \otimes \cdots \otimes |\psi_n\rangle$.*

Sistemas quânticos apresentam a possibilidade de criar correlações não locais a partir de iterações entre os sistemas isolados, o que não é possível realizar em sistemas clássicos. Tal correlação é chama de emaranhamento. Um estado $|\psi\rangle$ pertencente ao sistema composto $\mathcal{H}_A \otimes \mathcal{H}_B$ é dito emaranhado caso não possa ser escrito como o produto tensorial de estados pertencentes aos sistemas isolados $\mathcal{H}_A$ e $\mathcal{H}_B$, i.e., $\hat{\rho}_{AB} \in \mathcal{D}(\mathcal{H}_A \otimes \mathcal{H}_B)$ está emaranhado se não puder ser escrito como $\hat{\rho}_A \otimes \hat{\rho}_B$. Um exemplo de estado emaranhado é o estado de Bell $|\Psi^+\rangle_{AB} = (|00\rangle + |11\rangle)/\sqrt{2}$.

A.2 Sistemas de Variáveis Contínuas

Um sistema quântico cujo espaço de estados é um espaço de Hilbert de *dimensão infinita* é chamado de sistema quântico de variáveis contínuas (ou bosônico[1]) e tem como protótipo N osciladores harmônicos quânticos correspondendo aos N modos quantizados de campo da onda eletromagnética [64]. Essencialmente, cada modo do sistema é representado por um espaço de Hilbert $\mathcal{H}$ de dimensão infinita e todos os modos são associados pelo produto tensorial $\mathcal{H}^{\otimes N} = \otimes_{i=1}^{N} \mathcal{H}_i$, o qual representa o sistema completo, e tem associados os N pares de operadores bosônicos de campo $\{\hat{a}_1, \hat{a}_1^\dagger\}_{i=1}^{N}$ correspondentes, arranjados vetorialmente como $\hat{\boldsymbol{b}} = (\hat{a}_1, \hat{a}_1^\dagger, \cdots, \hat{a}_N, \hat{a}_N^\dagger)^T$, que deve satisfazer à seguinte relação de comutação bosônica

$$[\hat{b}_i, \hat{b}_j] = \Omega_{ij}, \quad (i, j = 1, 2, \cdots 2N), \tag{A.12}$$

[1]Bósons são partículas que se comportam estatisticamente de acordo com a distribuição de Bose-Einstein. Um exemplo comum desse tipo de partículas são os fótons.

sendo Ω_{ij} um elemento da matriz de forma simplética

$$\mathbf{\Omega} = \bigoplus_{k=1}^{N} \omega = \begin{pmatrix} \omega & & \\ & \ddots & \\ & & \omega \end{pmatrix}, \quad \omega = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}. \tag{A.13}$$

Como cada modo é composto por uma base ortonormal finita e contável $\{|n\rangle\}_{i=1}^{N}$, chamada de base de Fock (ou estados de número), o sistema de variáveis contínuas é separável. Os estados de número são particularmente associados com o operador de número $\hat{n} := \hat{a}^\dagger \hat{a}$ uma vez que são seus autovalores, $\hat{n}\,|n\rangle = n\,|n\rangle$, e, por consequência, relacionados aos operadores bosônicos da seguinte maneira,

$$\hat{a}\,|n\rangle = \sqrt{n}\,|n-1\rangle\,, \quad (n \geq 1), \quad \hat{a}\,|0\rangle = 0, \tag{A.14}$$

$$\hat{a}^\dagger\,|n\rangle = \sqrt{n+1}\,|n+1\rangle\,, \quad (n \geq 0), \tag{A.15}$$

sendo $|0\rangle$ o estado de vácuo, ou seja, a ausência de fótons no sistema.

Apesar de os operadores bosônicos descreverem completamente o sistema quântico, eles não são operadores hermitianos ($\hat{a} \neq \hat{a}^\dagger$)), resultando que não são observáveis do sistema. Entretanto, é possível obter operadores hermitianos derivados da decomposição cartesiana dos operadores bosônicos que irão também descrever o sistema quântico e são conhecidos como os operadores de quadratura de campo

$$\hat{q}_i := \hat{a}_i + \hat{a}_i^\dagger \qquad\qquad \hat{p}_i := i(\hat{a}_i^\dagger - \hat{a}_i), \tag{A.16}$$

os quais são uma analogia direta dos operadores de momento e posição de um oscilador harmônico quântico ideal, tendo um arranjo vetorial $\hat{\boldsymbol{r}} = (\hat{q}_1, \hat{p}_1, \cdots, \hat{q}_N, \hat{p}_N)^T$, respeitando a relação de comutação

$$[\hat{r}_i, \hat{r}_j] = 2i\Omega_{ij}, \quad (i, j = 1, 2, \cdots 2N), \tag{A.17}$$

a qual é derivada da Equação (A.12).

Outra possível descrição de estados quânticos são os momentos estatísticos. Em particular, os momentos estatísticos de sistemas quânticos com espectro contínuo são bastante úteis uma vez que permitem expressões simples para o cálculo de medidas de informação e de distância entre estados quânticos. Para um dado estado quântico $\hat{\rho}$, o primeiro momento é chamado de vetor de deslocamento e representa o valor esperado dos operadores de quadratura $\hat{q}$ e $\hat{p}$,

$$\bar{\boldsymbol{r}} := \langle \hat{\boldsymbol{r}} \rangle = \mathrm{tr}(\hat{\boldsymbol{r}}\hat{\rho}); \tag{A.18}$$

enquanto segundo momento é a matriz de covariância $\boldsymbol{V}$ cujos elementos são calculados de acordo com

$$V_{ij} = \frac{1}{2}\left\langle \{\Delta\hat{r}_i, \Delta\hat{r}_j\}\right\rangle, \tag{A.19}$$

sendo $\Delta\hat{r}_i = \hat{r}_i - \langle\hat{r}_i\rangle$ e $\{,\}$ o *anticomutador*.

A matriz de covariância é simplética de dimensão $2N \times 2N$ real, simétrica e positiva definida que descreve as correlações dos modos de quadratura e satisfaz o princípio da incerteza,

$$\boldsymbol{V} + i\boldsymbol{\Omega} \geq \boldsymbol{0}, \tag{A.20}$$

e que pode ser utilizada para derivar o princípio da incerteza na sua forma usual:

$$V(\hat{q}_i)V(\hat{p}_i) \geq 1. \tag{A.21}$$

Caso os termos relacionando aos operadores de quadratura $\hat{q}$ e $\hat{p}$ de diferentes modos sejam nulos, esses dois modos são descorrelacionados, implicando separabilidade [59]. Os momentos apresentados, vetor de deslocamento e matriz de covariância, são de grande importância uma vez que descrevem completamente os estados quânticos que fazem parte da classe de estados gaussianos: estados cuja representação de Wigner[2] é gaussiana. Estados gaussianos serão então denotados por $\hat{\rho}(\bar{\boldsymbol{r}}, \boldsymbol{V})$, sendo $\bar{\boldsymbol{r}}$ e $\boldsymbol{V}$ seu dois primeiros momentos estatísticos.

A.2.1 Operações Gaussianas

As operações quânticas modelam a evolução de um estado quântico por meio de um mapa linear $\mathcal{E} : \hat{\rho} \to \mathcal{E}(\hat{\rho})$, que é completamente positivo e no caso de preservação de traços ($\mathrm{tr}(\mathcal{E}(\hat{\rho})) = 1$) também é chamado de canal quântico. Quando um canal quântico é reversível, ele é representado por uma transformação unitária $\hat{U}$, $\hat{U}^{-1} = \hat{U}^T$. Então, dentro deste escopo, dizemos que uma operação quântica completamente positiva e que preserva o traço é gaussiana quando transforma estados gaussianos em estados gaussianos. Tais unidades são geradas por meio de um Hamiltoniano $\hat{H}$ que são polinômios de segunda ordem nos operadores canônicos, $\hat{U} = \exp\left\{-i\hat{H}/2\right\}$ e têm a forma geral

$$\hat{H} = i(\hat{\boldsymbol{a}}^\dagger\boldsymbol{\alpha} + \hat{\boldsymbol{a}}^{\dagger\boldsymbol{T}}\boldsymbol{A}\hat{\boldsymbol{a}} + \hat{\boldsymbol{a}}^{\dagger\boldsymbol{T}}\boldsymbol{B}\hat{\boldsymbol{a}}^\dagger) + \mathrm{H.\,c.}, \tag{A.22}$$

onde $\boldsymbol{\alpha} \in \mathbb{C}^N$, $\hat{\boldsymbol{a}} = (\hat{a}_1, \cdots, \hat{a}_N)^T$ é o vetor de operadores de aniquilação, $\boldsymbol{A}$ e $\boldsymbol{B}$ são $N \times N$ são matrizes simétricas complexas e Hc indica o conjugado hermitiano. Essa operação unitária corresponde à seguinte transformação de Bogoliubov na interpretação de Heisenberg

$$\hat{\boldsymbol{a}} \to \hat{\boldsymbol{b}} = \hat{U}^\dagger\hat{\boldsymbol{a}}\hat{U} = \boldsymbol{E}\hat{\boldsymbol{a}} + \boldsymbol{F}\hat{\boldsymbol{a}}^\dagger + \boldsymbol{\alpha}, \tag{A.23}$$

[2] A função de Wigner será tratada durante as estatísticas de detecção de quadratura, Apêndice A.3.2.

sendo $\boldsymbol{E}$ e $\boldsymbol{F}$ matrizes complexas que satisfazem as restrições $\boldsymbol{E}\boldsymbol{F}^T = \boldsymbol{F}\boldsymbol{E}^T$ e $\boldsymbol{E}\boldsymbol{E}^\dagger = \boldsymbol{F}\boldsymbol{F}^\dagger + \boldsymbol{I}$, chamadas de matrizes de Bogoliubov, e $\hat{\boldsymbol{b}}$ o vetor de operadores de aniquilação no campo de saída. A evolução unitária de ambos os operadores de criação e aniquilação na estrutura de Heisenberg pode ser arranjada na seguinte forma de matriz de bloco

$$\begin{pmatrix} \hat{\boldsymbol{a}} \\ \hat{\boldsymbol{a}}^\dagger \end{pmatrix} \to \begin{pmatrix} \hat{\boldsymbol{b}} \\ \hat{\boldsymbol{b}}^\dagger \end{pmatrix} = \begin{pmatrix} \boldsymbol{E} & \boldsymbol{F} \\ \boldsymbol{F}^* & \boldsymbol{E}^* \end{pmatrix} \begin{pmatrix} \hat{\boldsymbol{a}} \\ \hat{\boldsymbol{a}}^\dagger \end{pmatrix} + \begin{pmatrix} \boldsymbol{\alpha} \\ \boldsymbol{\alpha}^* \end{pmatrix}. \tag{A.24}$$

Analogamente à transformação de Bogouliubov, que relaciona os operadores canônicos de campo de entrada e saída, podemos definir uma descrição mais simples da unitária gaussiana por meio da evolução dos operadores de quadratura por um mapa afim

$$\hat{\boldsymbol{r}} \to \boldsymbol{S}\hat{\boldsymbol{r}} + \boldsymbol{d}, \tag{A.25}$$

onde $\boldsymbol{S}$ é uma matriz simplética $2N \times 2N$ real e $\boldsymbol{d} \in \mathbb{R}^{2N}$. Dada a relação direta entre os operadores canônicos bosônicos e os operadores de posição e momento, é possível recuperar $\boldsymbol{S}$ se $\boldsymbol{E}$ e $\boldsymbol{F}$ forem dados, e *vise-versa*.

A.2.2 Operações Fundamentais

Destacamos três operações unitárias Gaussianas específicas, a saber, os operadores deslocamento, compressão e rotação, que fatoram qualquer operador unitário Gaussiano arbitrário.

i) O deslocamento de N-modos é dado pelo operador

$$\hat{D}_{\boldsymbol{\alpha}} = \exp\big(\boldsymbol{\alpha}^T\hat{\boldsymbol{a}}^\dagger - \boldsymbol{\alpha}^\dagger\hat{\boldsymbol{a}}\big), \tag{A.26}$$

em que $\boldsymbol{\alpha} = (\alpha_1, \cdots, \alpha_N)^T \in \mathbb{C}^N$ e $\alpha_i = q_i + ip_i$. As respectivas matrizes de Bogoliubov são $\boldsymbol{E} = \boldsymbol{I}$ e $\boldsymbol{F} = \boldsymbol{0}$ com vetor de deslocamento $\boldsymbol{\alpha}$. Ainda mais, a operação simplética nos operadores de quadratura é dada por

$$\hat{\boldsymbol{r}} \to \hat{\boldsymbol{r}} + \boldsymbol{d}_\alpha, \qquad\qquad \boldsymbol{d}_\alpha = (q_1, p_1, \cdots, q_N, p_N)^T. \tag{A.27}$$

Para o caso especial do operador de deslocamento de um modo, sendo $\boldsymbol{\alpha} = \alpha \in \mathbb{C}$, utilizaremos a notação $\hat{D}_A(\alpha)$ para indicar o pertencimento ao modo do sistema A e o índice do modo será omitido sempre que estiver implícito no contexto.

ii) O operador de rotação em N-modos é especificado pela matriz $\boldsymbol{\phi}$ hermitiana e de dimensão $N \times N$,

$$\hat{R}_{\boldsymbol{\phi}} = \exp\big(i\hat{\boldsymbol{a}}^{\dagger\boldsymbol{T}}\boldsymbol{\phi}\hat{\boldsymbol{a}}\big), \tag{A.28}$$

que corresponde às matrizes de Bogoliubov $\boldsymbol{E} = e^{i\boldsymbol{\phi}}$ e $\boldsymbol{F} = \boldsymbol{0}$, com vetor de deslocamento nulo.

iii) O operador de compressão de N modos generalizado é definido pela matriz simétrica $\boldsymbol{Z}$ com dimensão $N \times N$

$$\hat{S}_{\boldsymbol{Z}} = \exp\left(\frac{1}{2}(\hat{\boldsymbol{a}}^{\dagger \boldsymbol{T}} \boldsymbol{Z} \hat{\boldsymbol{a}}^{\dagger} - \hat{\boldsymbol{a}}^{\boldsymbol{T}} \boldsymbol{Z}^{\dagger} \hat{\boldsymbol{a}})\right). \tag{A.29}$$

A matriz de compressão $\boldsymbol{Z}$ pode ser decomposta na forma polar $\boldsymbol{Z} = \boldsymbol{r}e^{i\boldsymbol{\theta}}$. Então, as matrizes de Bogoliubov são $\boldsymbol{E} = \cosh(\boldsymbol{r})$ e $\boldsymbol{F} = \sinh(\boldsymbol{r})e^{i\boldsymbol{\theta}}$. Analogamente ao operador de deslocamento, utilizaremos notações especiais para os casos de operadores de compressão de um e dois modos, conforme apresentaremos nas definições dos estados comprimidos de um e dois modos.

Os operadores unitários fundamentais não possuem a conveniência de serem mutuamente comutantes, mas, de acordo com [122], eles podem ser devidamente comutados com os devidos ajustes de parâmetros, conforme as *regras de comutação*:

$$\hat{D}_{\boldsymbol{\alpha}} \hat{S}_{\boldsymbol{Z}} = \hat{S}_{\boldsymbol{Z}} \hat{D}_{\boldsymbol{\beta}}, \qquad \boldsymbol{\beta} = \cosh(\boldsymbol{r})\boldsymbol{\alpha} - \sinh(\boldsymbol{r})e^{i\boldsymbol{\theta}}\boldsymbol{\alpha}^{*}, \tag{A.30}$$

$$\hat{S}_{\boldsymbol{Z}} \hat{R}_{\boldsymbol{\phi}} = \hat{R}_{\boldsymbol{\phi}} \hat{S}_{\boldsymbol{Z'}}, \qquad \boldsymbol{Z'} = e^{-i\boldsymbol{\phi}} \boldsymbol{Z} e^{-i\boldsymbol{\phi}^{T}}, \tag{A.31}$$

$$\hat{D}_{\boldsymbol{\alpha}} \hat{R}_{\boldsymbol{\phi}} = \hat{R}_{\boldsymbol{\phi}} \hat{D}_{\boldsymbol{\gamma}}, \qquad \boldsymbol{\gamma} = e^{-i\boldsymbol{\phi}} \boldsymbol{\alpha}. \tag{A.32}$$

Alguns estados gaussianos são de interesse fundamental em aplicações de teoria de informação quântica de variáveis contínuas. Trataremos especialmente de estados e operadores de um ou dois modos, sendo eles os estados de vácuo, térmico, coerentes e comprimidos. O estado de vácuo $|0\rangle$ é compreendido como o autoestado do operador de número com energia nula, $\hat{n}\,|0\rangle = 0$. Sua matriz de covariância é a identidade, significando que, apesar da ausência de fótons no sistema em estado de vácuo, os operadores de quadratura tem variância não nula, igual à unidade, o que significa que o estado de vácuo alcança simetricamente a incerteza mínima para observáveis não comutáveis. Essa variância mínima é conhecida como *ruído de fundo de vácuo* (*quantum shot noise*).

Definição A.7 (Estado Térmico)**.** *É chamado de térmico o estado de um sistema em equilíbrio térmico com energia média $\bar{n}$ tendo a seguinte representação na base de Fock,*

$$\hat{\rho}^{th}(\bar{n}) = \sum_{n=0}^{\infty} \frac{\bar{n}^{n}}{(\bar{n}+1)^{n+1}} \,|n\rangle\langle n|\,, \tag{A.33}$$

e momentos

$$\bar{\boldsymbol{r}}_{th} = (0,0)^{T} \qquad \boldsymbol{V}_{th}(\bar{n}) = \begin{pmatrix} (2\bar{n}+1) & 0 \\ 0 & (2\bar{n}+1). \end{pmatrix}. \tag{A.34}$$

O estado térmico é associado ao sistema quântico que está maximamente misturado [123, 124] e é o estado gaussiano que, para um nível fixo de energia, maximiza a entropia de von Neumann.

Definição A.8 (Estado Coerente)**.** *A operação de deslocamento de um modo em um estado de vácuo produz o estado coerente,*

$$|\alpha\rangle = \hat{D}(\alpha)\,|0\rangle\,, \tag{A.35}$$

sendo $\alpha = q + ip$ a amplitude complexa do estado coerente, e no espaço de fase com os dois primeiros momentos

$$\bar{\boldsymbol{r}}_{cs} = (q, p)^T \qquad\qquad \boldsymbol{V}_{cs} = \begin{pmatrix} 1 & 0 \\ 0 & 1. \end{pmatrix}. \tag{A.36}$$

Os estados coerentes, como pode ser observado na sua matriz de covariância, apresentam a incerteza mínima em ambas as quadraturas. Utilizando a ordenação normal do operador de deslocamento ($\hat{D}(\alpha) = e^{-|\alpha|^2/2} : \hat{D}(\alpha) :$), juntamente com a expansão de operadores em série de potências, é possível obter a representação dos estados coerentes na base de Fock:

$$|\alpha\rangle = e^{-|\alpha|^2/2} \sum_{n=0}^{\infty} \frac{\alpha^n}{\sqrt{n!}}\,|n\rangle\,. \tag{A.37}$$

Algumas características dos estados coerentes podem ser destacadas. A primeira é sua não ortogonalidade. De fato, para $\alpha, \beta \in \mathbb{C}$, temos que

$$\langle\beta|\alpha\rangle = \exp\{(\beta^*\alpha - \beta\alpha^*)/2\}\exp\{-|\beta - \alpha|^2/2\}, \tag{A.38}$$

do que seque a interseção entre dois estados coerentes nunca é nula mas é inversamente proporcional ao valor absoluto da diferença de suas amplitudes. Apesar de não serem ortogonais, estados coerentes obedecem a relação de completude, ou seja, resolvem a identidade,

$$\hat{I} = \int_{\mathbb{C}} \frac{\mathrm{d}^2\alpha}{\pi}\,|\alpha\rangle\langle\alpha|\,, \tag{A.39}$$

de modo que são caracterizados por formarem uma *base supercompleta*, sendo $\hat{I}$ o operador identidade do espaço. De sua característica de ser uma base supercompleta, segue que é possível calcular o traço de um operador qualquer (digamos, $\hat{A}$) como uma integração no plano complexo:

$$\mathrm{tr}(\hat{A}) = \mathrm{tr}(\hat{A}\hat{I}) = \mathrm{tr}\left[\hat{A}\int_{\mathbb{C}} \frac{\mathrm{d}^2\alpha}{\pi}\,|\alpha\rangle\langle\alpha|\right] = \int_{\mathbb{C}} \frac{\mathrm{d}^2\alpha}{\pi}\,\langle\alpha|\hat{A}|\alpha\rangle \tag{A.40}$$

Como último uso da base *supercompleta* que os estados coerentes formam, é útil pontuar que é possível utilizar o processo de ortogonalização de Grahm-Schmidt para obter uma base ortonormal a partir de um conjunto finito de estados coerentes. Vamos definir um conjunto arbitrário de estados $\mathcal{S} = \{|\alpha_i\rangle\}_{i=0}^{K-1}$ em que $\alpha_i \in \mathbb{C}$. Dos estados em $\mathcal{S}$ podemos construir a matriz de produtos internos $\boldsymbol{V}_{\mathcal{S}}$ cujos elementos arbitrários são

$$V_{ij} = \langle \alpha_i | \alpha_j \rangle = e^{\frac{1}{2}(\alpha_i^* \alpha_j - \alpha_i \alpha_j^*)} e^{-\frac{1}{2}|\alpha_i - \alpha_j|^2}. \tag{A.41}$$

Utilizando o processo de ortogonalização de Gram-Schmidt podemos construir a partir de $\mathcal{S}$ uma base orthonormal $\mathcal{B} = \{|\psi_0\rangle, \cdots, |\psi_{K-1}\rangle\}$ que será uma base para o subespaço gerado pelo conjunto $\{|\alpha_i\rangle\}_{i=0}^{K-1}$ que podem ser decompostos da seguinte forma:

$$|\alpha_k\rangle = \sum_{i=0}^{K-1} \langle \psi_i | \alpha_k \rangle |\psi_i\rangle = \sum_{i=0}^{K-1} M_{ki} |\psi_i\rangle, \tag{A.42}$$

em que $M_{k,i}$ corresponde à projeção do k-ésimo estado $|\alpha_k\rangle$ no i-ésimo elemento da base $\mathcal{B}$. As projeções são arranjadas na matriz $\boldsymbol{M}$, cujos elementos podem ser calculados conforme o seguinte elemento

$$M_{k0} = V_{0k} \tag{A.43}$$

$$M_{ki} = \begin{cases} \frac{1}{M_{ii}}(V_{ik} - \sum_{j=0}^{i-1} M_{ij}^* M_{kj}), & \text{se } 1 \leq i < k, \\ 0, & \text{se } i > k, \end{cases} \tag{A.44}$$

$$M_{kk} = \left(1 - \sum_{i=0}^{k-1} |M_{ki}|^2\right)^{\frac{1}{2}} \quad \text{para } k > 0. \tag{A.45}$$

Definição A.9 (Operador de Compressão e Estado Comprimido)**.** *A aplicação do operador de compressão de um modo* $\hat{S}(\xi) = \exp\big(\xi(\hat{a}^2 - \hat{a}^{\dagger 2})/2\big)$*, com* $\xi = re^{i\phi}$*,* $r < \infty$ *e* $0 \leq \phi < 2\pi$*, no estado de vácuo produz o estado de vácuo comprimido*

$$|\xi\rangle = \hat{S}(\xi)|0\rangle = \frac{1}{\sqrt{\cosh r}} \sum_{n=0}^{\infty} \frac{\sqrt{(2n)!}}{2^n n!} \big(-e^{i\phi} \tanh r\big)^n |2n\rangle. \tag{A.46}$$

Claramente os estados de vácuo comprimido apresentam produto mínimo de incerteza de quadratura. Em particular, é de interesse o estado térmico após a operação de compressão de quadratura. Fazendo $r = -\ln\sqrt{2\bar{n}+1}$ e $\phi = 0$ temos que $\hat{S}(\xi)$ realiza o mapeamento simplético de acordo com a matriz $\mathrm{diag}(e^{-r}, e^{r})$ e que a matriz de covariância do estado térmico $\hat{\rho}^{th}(\bar{n})$ é transformada para

$$\boldsymbol{S}(r)\boldsymbol{V}_{th}(\bar{n})\boldsymbol{S}(r) = \begin{pmatrix} (2\bar{n}+1)^2 & 0 \\ 0 & 1 \end{pmatrix}, \tag{A.47}$$

e o vetor de média não sofre alteração.

Definição A.10 (Estado de Vácuo Comprimido de Dois Modos)**.** *Quando um cristal no regime OPA não degenerado é atingido por um laser são gerados fótons em dois modos distintos, chamados de modo do sinal e modo ocioso. Essa operação é a compressão de dois modos com operador unitário dado por*

$$\hat{S}_2(z) = \exp\Big\{\frac{z}{2}(\hat{a}\hat{b} - \hat{a}^\dagger\hat{b}^\dagger)\Big\}, \tag{A.48}$$

e a matriz simplética correspondente a $\hat{S}_2(z)$ *é*

$$\boldsymbol{S}_2(z) = \begin{pmatrix} \cosh(z)\boldsymbol{I} & \sinh(z)\boldsymbol{Z} \\ \sinh(z)\boldsymbol{Z} & \cosh(z)\boldsymbol{I} \end{pmatrix}. \tag{A.49}$$

Aplicando o operador $\hat{S}_2(z)$ *em um par de estados de vácuo é obtido o estado de vácuo comprimido de dois modos (TMSV), também conhecido como estado EPR (Einstein-Podolski-Rosen),*

$$|z\rangle_{EPR} = \hat{S}_2(z)\,|0\rangle_a\,|0\rangle_b = \sqrt{1-\lambda^2}\sum_{n=0}^{\infty}(-\lambda)^n\,|n\rangle_a\,|n\rangle_b\,, \tag{A.50}$$

sendo $\lambda = \tanh(z)$*.*

O estado TMSV é um estado gaussiano com média nula e matriz de covariância

$$\boldsymbol{V}_{EPR} = \begin{pmatrix} \nu\boldsymbol{I} & \sqrt{\nu^2-1}\boldsymbol{Z} \\ \sqrt{\nu^2-1}\boldsymbol{Z} & \nu\boldsymbol{I}, \end{pmatrix} \tag{A.51}$$

em que $\nu = \cosh(2z)$ corresponde à *variância de ruído das quadraturas.*

Definição A.11 (Divisor de Feixe)**.** *O divisor de feixe é uma operação gaussiana de dois modos definida pelo operador unitário*

$$\hat{B}(\theta) = \exp\Big\{\theta(\hat{a}^\dagger\hat{b} - \hat{a}\hat{b}^\dagger)\Big\}, \tag{A.52}$$

em que $\hat{a}$ *e* $\hat{b}$ *são operadores de aniquilação dos modos de entrada do divisor e a constante* θ *determina a transmissividade do dispositivo como* $\tau = \cos^2(\theta)$*. A atuação do BS nos modos incidentes realiza as seguintes transformações de operadores*

$$\begin{pmatrix} \hat{a} \\ \hat{b} \end{pmatrix} \to \begin{pmatrix} \sqrt{\tau} & \sqrt{1-\tau} \\ -\sqrt{1-\tau} & \sqrt{\tau} \end{pmatrix} \begin{pmatrix} \hat{a} \\ \hat{b} \end{pmatrix} \tag{A.53}$$

e possui matriz simplética

$$\boldsymbol{B}(\tau) = \begin{pmatrix} \sqrt{\tau}\boldsymbol{I} & \sqrt{1-\tau}\boldsymbol{I} \\ -\sqrt{1-\tau}\boldsymbol{I} & \sqrt{\tau}\boldsymbol{I} \end{pmatrix}. \tag{A.54}$$

Exemplo A.12 (Interferência entre um estado coerente e de vácuo)**.** *Vamos considerar um sistema de dois modos, A e B, em que o primeiro modo está em um estado de vácuo e o segundo em um coerente $|\alpha\rangle$, e que esses modos interagem por meio de um divisor de feixe, conforme a Figura 30. Utilizando a transformação de operadores realizada pela operação do BS, temos que os modos de saída estão relacionados aos modos de entrada da seguinte maneira*

$$\hat{a} \xrightarrow{\hat{B}} \hat{c} = t\hat{a} + r\hat{b} \tag{A.55}$$

$$\hat{b} \xrightarrow{\hat{B}} \hat{d} = -r\hat{a} + t\hat{b}, \tag{A.56}$$

$$\tag{A.57}$$

em que $t = \sqrt{\tau}$ e $r = \sqrt{1-\tau}$. Dado que o estado do sistema composto pode ser escrito como $|\alpha\rangle_A |0\rangle_B = \hat{D}_A(\alpha) |0\rangle_A |0\rangle_B$ e que os operadores canônicos dos modos de entrada estão relacionados aos modos de saída como

$$\hat{a} = t\hat{c} - r\hat{d} \tag{A.58}$$

$$\hat{b} = r\hat{c} + t\hat{d}, \tag{A.59}$$

segue que

$$\hat{B} |\alpha\rangle_A |0\rangle_B = \hat{B}\hat{D}(\alpha) |00\rangle_{AB} = \hat{B} \exp\{\alpha\hat{a}^\dagger - \alpha^*\hat{a}\} |00\rangle_{AB} \tag{A.60}$$

$$= \exp\Big\{\alpha(t\hat{c}^\dagger - r\hat{d}^\dagger) - \alpha^*(t\hat{c} - r\hat{d})\Big\} |00\rangle_{CD} \tag{A.61}$$

$$= \exp\{t\alpha\hat{c}^\dagger - t\alpha^*\hat{c}\} \exp\Big\{r\alpha\hat{d}^\dagger - r\alpha^*\hat{d}\Big\} |00\rangle_{CD} \tag{A.62}$$

$$= \hat{D}(t\alpha) |0\rangle_C \hat{D}(-r\alpha) |0\rangle_D \tag{A.63}$$

$$= |\sqrt{\tau}\alpha\rangle_C |-\sqrt{1-\tau}\alpha\rangle_D . \tag{A.64}$$

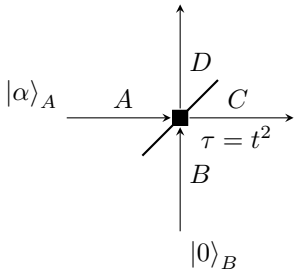


Figura 30 – Interferência entre um estado coerente e um estado de vácuo por meio de um divisor de feixe com transmissividade τ.

A.3 Estatística de Detecção de Quadratura

Para iniciar a discussão de estatísticas de fotodetecção, partiremos da descrição clássica de funções características de uma variável aleatória contínua. A análise realizada segue o modelo de [125].

A.3.1 Função Característica Quântica

A função característica de uma variável aleatória X é descrita como

$$M_X(jv) := \left\langle e^{jvX} \right\rangle = \int_{-\infty}^{\infty} dx e^{jvx} p_X(x), \tag{A.65}$$

de modo que a função densidade de probabilidade é dada por

$$p_X(x) = \int_{-\infty}^{\infty} \frac{dv}{2\pi} M_X(jv) e^{-jvx}, \tag{A.66}$$

estando $M_X(jv)$ e $p_X(x)$ relacionados como um par de transformadas de Fourier[3].

Como o resultado da medição de estado quânticos são valores reais e não operadores lineares no espaço do sistema, a pergunta a ser respondida é: qual o comportamento estatístico da variável aleatória oriunda da medição realizada por Bob quando ele recebe um estado enviado por Alice? De modo geral, o procedimento a ser modelado estatisticamente (e objetivo de Bob) é realizar a detecção do operador de quadratura $\hat{a}(t)$, o operador que contém informação de ambas as quadraturas do estado transmitido. A metodologia geral consiste em usar funções características para determinar o comportamento estatístico das medições.

Seja $\hat{a}(t)$ o operador de aniquilação do modo transmitido por Alice no tempo t e suas partes real e imaginária

$$\hat{a}_1(t) = \mathrm{Re}\{\hat{a}(t)\}, \qquad \hat{a}_2(t) = \mathrm{Im}\{\hat{a}(t)\}, \tag{A.67}$$

e $a_1(t)$ e $a_1(t)$ variáveis aleatórias correspondendo à medição das partes real e imaginária de $\hat{a}(t)$, respectivamente. Suponha que seja realizada a medição de $\hat{a}_1(t)$. A função característica clássica para $a_1(t)$ é dada por

$$M_{a_1(t)}(jv) = \left\langle e^{jva_1(t)} \right\rangle = \langle\psi| \left(e^{jv\hat{a}_1(t)}\right) |\psi\rangle = \left\langle e^{jv\hat{a}_1(t)} \right\rangle, \tag{A.68}$$

que é obtido utilizando a definição na Equação (A.65), as identidades[4] $p_{a_1(t)}(\alpha_1) = |\langle\psi|\alpha_1\rangle|^2 = \langle\psi|\alpha_1\rangle\langle\alpha_1|\psi\rangle$, a expansão em série de Taylor de $e^{jv\alpha_1}$ e usando

[3]Funções características são casos especiais das funções geradoras de momento, estas sendo relacionadas com os momentos de uma variável aleatória pela transformada de Laplace.

[4]Dado que estados coerentes formam uma base supercompleta, o operador $\hat{a}_1(t)$ pode ser decomposto em termos dos autoestados (estados coerentes) e autovalores α.

que α_1 é um autovalor de $\hat{a}_1(t)$. O resultado final é que a caracterização estatística da variável aleatória que representa a medição de um operador de quadratura é idêntica à do próprio operador:

$$\left\langle e^{jva_1(t)} \right\rangle \equiv \left\langle e^{jv\hat{a}_1(t)} \right\rangle . \tag{A.69}$$

A importância desse resultado reside no estabelecimento de uma equivalência entre o comportamento estatística de um operador quântico e o comportamento estatístico da variável aleatória que representa o resultado da medição deste operador. Enquanto o termo do lado esquerdo da Equação (A.69) é já conhecido, desenvolveremos o termo do lado direito, conhecido como Função Característica de Wigner (FCW):

Definição A.13 (Função Característica de Wigner)**.** *Seja $\zeta \in \mathbb{C}$ e ζ_1 e ζ_2 suas partes real e imaginária, respectivamente, $\mathcal{H}$ o espaço de Hilbert associado a um sistema quântico $\hat{\rho}$ e $\hat{a}$ o operador de aniquilação do sistema. A Função Característica de Wigner de um operador $\hat{a}$ com relação ao estado $\hat{\rho}$ é definida como*[5]

$$\chi_W(\zeta^*, \zeta) := \mathrm{tr}(\hat{\rho}\hat{D}(\zeta)) = \left\langle e^{-\zeta^*\hat{a}+\zeta\hat{a}^\dagger} \right\rangle , \tag{A.70}$$

sendo $\hat{D}(\zeta)$ o operador de deslocamento de um modo.

Fazendo uso da Equação (A.67) é possível reescrever a Equação (A.70) como

$$\chi_W(\zeta^*, \zeta) = \left\langle e^{-2j\,\mathrm{Im}\{\zeta^*\hat{a}\}} \right\rangle , \tag{A.71}$$

seguindo que

$$M_{a_1(t)}(jv) = \chi_W(\zeta^*, \zeta)\Big|_{\zeta = jve^{j v\omega t/2}} . \tag{A.72}$$

Em diversos casos, para cálculo das funções características de Wigner, é comum utilizar as representações nas formas ordenadas e não-ordenadas, as quais são obtidas pela decomposição de uma função exponencial de soma de operadores lineares a partir do Teorema de Baker–Campbell–Hausdorff (BCH):

Teorema A.14. *Sejam $\hat{A}$ e $\hat{B}$ operadores lineares do espaço de Hilbert. Se $\hat{A}$ e $\hat{B}$ não comutam entre si mas comutam com seu comutador, então*

$$e^{\hat{A}+\hat{B}} = e^{\hat{A}}e^{\hat{B}}e^{-\left[\hat{A},\hat{B}\right]/2} = e^{\hat{B}}e^{\hat{A}}e^{\left[\hat{A},\hat{B}\right]/2}. \tag{A.73}$$

Desta maneira, a FCW pode ser reescrita como

$$\chi_W(\zeta^*, \zeta) = \left\langle e^{-\zeta^*\hat{a}+\zeta\hat{a}^\dagger} \right\rangle = \left\langle e^{-\zeta^*\hat{a}}e^{\zeta\hat{a}^\dagger} \right\rangle e^{|\zeta|^2/2} = \chi_A(\zeta^*, \zeta)e^{|\zeta|^2/2} \tag{A.74}$$

[5] A função de Wigner é generalizável para N modos arbitrários, bastando considerar o operador de deslocamento de N modos.

$$= \left\langle e^{\zeta \hat{a}^\dagger} e^{-\zeta^* \hat{a}} \right\rangle e^{-|\zeta|^2/2} = \chi_N(\zeta^*, \zeta) e^{-|\zeta|^2/2}, \tag{A.75}$$

em que $\chi_A(\zeta^*, \zeta)$ e $\chi_N(\zeta^*, \zeta)$ são as funções características quânticas *anti*-normalmente e normalmente ordenadas. A ordenação e normal e anti-normal está relacionada com a ordem dos operadores de aniquilação, e se aplicam em qualquer representação de operadores quânticos. Como a função característica para $a_i(t)$ é equivalente à FCW de $\hat{a}_1(t)$ para $\zeta = jve^{j\omega t/2}$, segue que

$$M_{a_1(t)}(jv) = \chi_W(\zeta^*, \zeta)\Big|_{\zeta = jve^{jv\omega t/2}} = \chi_N(\zeta^*, \zeta) e^{-|\zeta|^2/2}\Big|_{\zeta = jve^{jv\omega t/2}}. \tag{A.76}$$

Logo, a função densidade de probabilidade da variável aleatória associada à medição de um operador quântico é obtida a partir da transformada inversa de Fourier da FCW do operador, justificado pela Equação (A.69):

$$p_{a_1(t)}(\alpha_1) = \frac{1}{2\pi} \int_{-\infty}^{\infty} \mathrm{d}v \, M_{a_1(t)}(jv) e^{-jv\alpha_1} \tag{A.77}$$

A.3.2 Distribuição de Probabilidade de Wigner

Os resultados obtidos na Seção anterior apresentam a utilização da FCW para chegar à função densidade de probabilidade da variável de medição. Para tal, é utilizada a transformada inversa de Fourier de $M_{a_1(t)}(jv)$. O que ocorre é que $\chi_W(\zeta^*, \zeta)$ é uma função de duas variáveis, ζ_1 e ζ_2, enquanto $M_{a_1(t)}(jv)$ dá informação a respeito de uma única quadratura,

$$p_{a_1(t)}(\alpha_1) \underset{\mathcal{F}^{-1}}{\overset{\mathcal{F}}{\rightleftarrows}} M_{a_1(t)}(jv). \tag{A.78}$$

Desta maneira, o resultado obtido para $p_{a_1(t)}(\alpha_1)$ pode ser obtido, seguindo o mesmo procedimento, para $p_{a_2(t)}(\alpha_2)$, isso porque a χ_W detém informação a respeito de ambas as quadraturas do operador $\hat{a}(t)$. A maneira de realizar uma transformação da FCW que preserve informação a respeito de ambas as quadraturas de $\hat{a}(t)$ é por meio da trasformada bidimensional de Fourier da Função Característica de Wigner, conhecida como a Distribuição de Wigner.

Definição A.15 (Distribuição de Wigner)**.** *Seja $\chi_W(\zeta^*, \zeta)$ uma FCW de um operador linear e $\alpha = \alpha_1 + j\alpha_2$, $\alpha 1, \alpha_2 \in \mathbf{R}$, a transformada inversa bidimensional de Fourrier de χ_W é chamada Distribuição de Wigner,*

$$W(\alpha, \alpha^*) = \int \frac{\mathrm{d}^2\zeta}{\pi^2} \chi_W(\zeta^*, \zeta) e^{\zeta^*\alpha - \zeta\alpha^*}, \tag{A.79}$$

Como a transformada inversa de Fourier de uma função característica é necessariamente uma função densidade de probabilidade e χ_W é uma função

característica de duas variáveis auxiliares, ζ_1 e ζ_2, $W(\alpha, \alpha^*)$ é uma função densidade de probabilidade conjunta das variáveis α_1 e α_2, e é estabelecido o par de transformadas (bidimensionais)

$$W(\alpha, \alpha^*) \underset{\mathcal{F}^{-1}}{\overset{\mathcal{F}}{\rightleftarrows}} \chi_W(\zeta^*, \zeta). \tag{A.80}$$

Exemplo A.16 (Distribuição de Wigner para estados coerentes)**.** *Para um sistema que está em um estado coerente $|\beta\rangle$ e tem operador de aniquilação associado $\hat{a}$, para obter a pdf conjunta de α_1 e α_2, é calculada a FCW,*

$$\chi_W(\zeta^*, \zeta) = \langle\beta| e^{\zeta \hat{a}^\dagger} e^{-\zeta^* \hat{a}} e^{-|\zeta|/2} |\beta\rangle \tag{A.81}$$

$$= e^{\zeta\beta^*} e^{-\zeta^*\beta} e^{-|\zeta|/2}. \tag{A.82}$$

A partir de $\chi_W(\zeta^*, \zeta)$, é calculada a distribuição de Wigner

$$W(\alpha, \alpha^*) = \int \frac{\mathrm{d}^2\zeta}{\pi^2} \chi_W(\zeta^*, \zeta) e^{\zeta^*\alpha - \zeta\alpha^*} \tag{A.83}$$

$$= \int \frac{\mathrm{d}^2\zeta}{\pi^2} e^{\zeta\beta^*} e^{-\zeta^*\beta} e^{-|\zeta|/2} e^{\zeta^*\alpha - \zeta\alpha^*} \tag{A.84}$$

$$= \frac{e^{-2|\alpha-\beta|^2}}{\pi/2} \tag{A.85}$$

A expressão obtida indica que α_1 e α_2 são variáveis aleatórias independentes com valores médios β_1 e β_2 e variâncias $\frac{1}{4}$.

A.3.3 Realização da Detecção

As equivalências estatísticas entre funções características clássicas e funções características de Wigner e as relações destas com funções de distribuição de probabilidades clássicas e a distribuição de Wigner desenvolvidas na seção anterior servirão de base para justificar e viabilizar um esquema de medição do operador de qudratura $\hat{a}$. O operador $\hat{a}$ pode ser compreendido como um POVM, uma classe de operadores de medição amplamente utilizados na teoria da informação quântica. Porém, devido à não hermiticidade do operador, não constitui um observável.

Estatística do POVM $\hat{a}$

O operador de quadratura $\hat{a}$ possui autoespectro contínuo e, sendo α os autovalores de $\hat{a}$ números complexos com partes real e imaginária α_1 e α_2, a função densidade de probabilidade $p(\alpha)$ de detecção de $\hat{a}$ é conjunta para cada quadratura, *i.e.*, uma função distribuição de probabilidades conjunta das variáveis aleatórias α_1 e α_2 com função

característica

$$M_{a_1a_2}(jv_1, jv_2) = \int \mathrm{d}\alpha_1 \int \mathrm{d}\alpha_2 \, e^{jv\alpha_1 + jv\alpha_2} \frac{\left|\langle\psi|\alpha\rangle\right|^2}{\pi}, \tag{A.86}$$

e distribuição de Wigner

$$\chi_A(\zeta^*, \zeta) = \langle\psi|e^{-\zeta^*\hat{a}} e^{\zeta^*\hat{a}^\dagger}|\psi\rangle = \int \mathrm{d}^2\alpha \, e^{-\zeta^*\alpha + \zeta^*\alpha^*} \frac{\left|\langle\psi|\alpha\rangle\right|^2}{\pi}. \tag{A.87}$$

Fazendo $v = v_1 + jv_2$ e $\zeta = \zeta_1 + j\zeta_2$,

$$M_{a_1a_2}(jv_1, jv_2) = \chi_A(\zeta^*, \zeta)\Big|_{\zeta=\frac{jv}{2}} \tag{A.88}$$

Entretanto, $\hat{a}$ não é hermitiano, logo, não é um observável. Contudo, é possível obter um observável por meio do acoplamento do sinal a ser medido com uma *ancilla* de modo que o operador do sistema resultante possa ser medido. Sejam $\mathcal{H}_S$, $|\psi\rangle_S$ e $\hat{a}_S$ o sistema, estado e operador de aniquilação associados ao sinal, respectivamente, e de modo análogo, $\mathcal{H}_A$, $|0\rangle_A$ e $\hat{a}_A$ com relação à *ancilla*. É possível definir um operador que atua no sistema composto $\mathcal{H}_S \otimes \mathcal{H}_A$

$$\hat{y} = \hat{a}_S \otimes \hat{I}_A + \hat{I}_S \otimes \hat{a}_A^\dagger, \tag{A.89}$$

de modo que, mesmo $\hat{y}$ não sendo hermitiano, comuta com seu adjunto[6],

$$\left[\hat{y}, \hat{y}^\dagger\right] = \left[\hat{a}_S \otimes \hat{I}_A, \hat{a}_S^\dagger \otimes \hat{I}_A\right] + \left[\hat{I}_S \otimes \hat{a}_A^\dagger, \hat{I}_S \otimes \hat{a}_A\right] = 0, \tag{A.90}$$

cujas partes real e imaginária são[7]

$$\hat{y}_1 = \hat{a}_{S_1} \otimes \hat{I}_A + \hat{I}_S \otimes \hat{a}_{A_1} \qquad \hat{y}_2 = \hat{a}_{S_2} \otimes \hat{I}_A - \hat{I}_S \otimes \hat{a}_{A_1}. \tag{A.91}$$

Os operadores $\hat{y}_1$ e $\hat{y}_2$ são observáveis, o que quer dizer que representam grandezas físicas mensuráveis, e comutam entre si, sendo possível realizar a medição simultânea de ambos os operadores.

Associadas a $\hat{y}_1$ e $\hat{y}_2$ estão as variáveis aleatórias y_1 e y_2, os resultados da medição dos operadores supracitados, respectivamente. Logo, é possível utilizar a equivalência entre a função característica clássica das variáveis aleatórias y_1 e y_2 e a FCW dos respectivos operadores, conforme obtido na Equação (A.69), relacionando o comportamento estatístico de y_1 e y_2 com os operadores $\hat{a}_S$ e $\hat{a}_S^\dagger$. Admitindo que o sistema do sinal está em um estado arbitrário $|\psi\rangle_S$ válido e que o sistema da *ancilla*

[6]Note que o comutador é distributivo, $[A+B, C+D] = [A,C] + [A,D] + [B,C] + [B,D]$, e que $\left[\hat{a}_S \otimes \hat{I}_A, \hat{I}_S \otimes \hat{a}_A\right] = 0$ e $\left[\hat{I}_S \otimes \hat{a}_A^\dagger, \hat{a}_S^\dagger \otimes \hat{I}_A\right] = 0$.

[7]Para tal, basta notar que $\hat{a}_S = \hat{a}_{S_1} + j\hat{a}_{S_2}$, sendo $\hat{a}_{S_1}$ $\hat{a}_{S_2}$ as partes reais e imaginárias do operador $\hat{a}_S$, respectivamente. O mesmo é realizado para $\hat{a}_A$, de maneira análoga.

encontra-se em um estado de vácuo, $|0\rangle_A$, a partir da função característica clássica conjunta de y_1 e y_2, temos que

$$\left\langle e^{jv_1y_1+jv_2y_2}\right\rangle = \left\langle e^{jv_1\hat{y}_1+jv_2\hat{y}_2}\right\rangle = \chi_{A_S}(\zeta^*,\zeta)\Big|_{\zeta=\frac{jv}{2}} \tag{A.92}$$

Então, é visto que o comportamento estatístico de y_1 e y_2 é idêntico ao dos operadores $\hat{a}_S$ e $\hat{a}_S^\dagger$. De fato, utilizando a Equação (A.88),

$$M_{y_1y_2}(jv_1,jv_2) = M_{a_1a_2}(jv_1,jv_2). \tag{A.93}$$

A.3.4 Esquemas de Detecção

Nas seções seguintes descreveremos a estatística de detecção direta de um estado quântico ótico, ou seja, contagem de fotos, e ainda como realizar o POVM que mede as quadraturas descritas por $\hat{a}$ e $\hat{a}^\dagger$.

Detecção Direta

O método de detecção direta consiste no processo de contagem direta de fótons incidindo em um fotodetector. A Fig. 31 apresenta o modelo de uma detecção direta ideal. Nele, o campo eletromagnético incide em um fotodetector ideal, o qual irá produzir uma fotocorrente $i(t)$ que é equivalente a um trem de pulsos aleatórios de área q (carga de um elétron). Sua eficiência unitária indica que cada fóton incidente na região ativa do fotodetector resulta em um impulso no trem de impulsos. Na segunda etapa da detecção direta é realizada a contagem de impulsos da fotocorrente dentro do período de detecção T, produzindo a variável aleatória $N(t)$. Neste caso, a contagem é normalizada com relação à carga do elétron, fazendo que a forma de $N(t)$ seja uma função escada com degraus unitário.

A teoria quântica de fotodetecção transforma o fasor de campo em um operador e o modelo de detecção direta será conforme a Figura 31. Logo, sendo o estado inicial do sistema incidente $|\psi\rangle$, a probabilidade de serem contados n fótons do modo incidente dado seu estado inicial é obtida pela expressão

$$\Pr = (N=n|\,\text{estado} = |\psi\rangle\langle\psi|) = |\langle n|\psi\rangle|^2. \tag{A.94}$$

Aqui, o procedimento de fotodetecção realiza a medição do operador de número $\hat{n}$, observável que representa o número de fótons do estado do sistema quântico. Para o caso

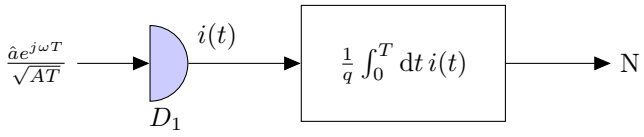


Figura 31 – Fotodetector ideal com área A ativa de detecção durante o período T.

do sistema estar em um estado coerente, é possível ver que a estatística de detecção do modelo quântico é equivalente ao modelo semiclássico,

$$\Pr = (N = n|\,\text{estado} = |\psi\rangle\langle\psi|) = |\langle n|\psi\rangle|^2 = \frac{|\alpha|^{2n}}{n!}e^{-|\alpha|^2}, \tag{A.95}$$

o que não se mantém para quando o sistema está em um estado de número, de modo que

$$\Pr = (N = n|\,\text{n'} = |\psi\rangle\langle\psi|) = |\langle n|n'\rangle|^2 = \delta_{nn'}. \tag{A.96}$$

Neste resultado é identificado o primeiro traço de não clássico dos estados de número ao apresentarem distribuição subpoisoniana[8].

Detecção Homódina

A detecção homódina é o primeiro método que realiza o acoplamento do sinal principal com um oscilador local (LO), neste caso, o oscilador estando na mesma frequência do sinal principal, justificando o nome. O Objetivo deste esquema é realizar a medição da quadratura referente à fase relativa θ entre o sinal e o LO, chamada de *quadratura* θ.

Neste esquema, descrito na Figura 32, o sinal e o LO são mixados por meio de um divisor de feixe balanceado, sem perdas, com matriz simplética conforme a Equação (A.54) com parâmetro $\tau = 1/2$. Os campos de saída de cada braço do BS são os campos do sinal e do LO acoplados, os quais incidem nos fotodetectores D_1 e D_2, respectivamente. Para análise da detecção homódina quântica, os operadores de campo $\hat{E}_S = \hat{a}_S e^{-j\omega}/\sqrt{AT}$ e $\hat{E}_{LO} = \hat{a}_{LO}e^{-j\omega}/\sqrt{AT}$ representam os modos do sinal principal e do escilador local, respectivamente, em que é admitido que o oscilador local está no estado coerente inicial $\left|\sqrt{N_{LO}}e^{j\theta}\right\rangle$ que satisfaz a seguinte condição $\langle n_S\rangle \ll \langle n_{LO}\rangle$. Os operadores de campo são transformados pelo divisor de feixe como

$$\begin{pmatrix}\hat{E}_+\\ \hat{E}_-\end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}\begin{pmatrix}\hat{E}_S\\ \hat{E}_{LO}\end{pmatrix} = \frac{1}{\sqrt{2}}\frac{e^{-j\omega t}}{\sqrt{AT}}\begin{pmatrix}\hat{a}_S + \hat{a}_{LO}\\ \hat{a}_S - \hat{a}_{LO}\end{pmatrix} = \frac{1}{\sqrt{2}}\frac{e^{-j\omega t}}{\sqrt{AT}}\begin{pmatrix}\hat{a}_+\\ \hat{a}_-\end{pmatrix}. \tag{A.97}$$

Devido à linearidade da operação de contagem de fótons, a detecção homódina realiza a diferença de contagem entre dois detectores diretos, referentes aos campos

[8] variância menor que valor esperado.

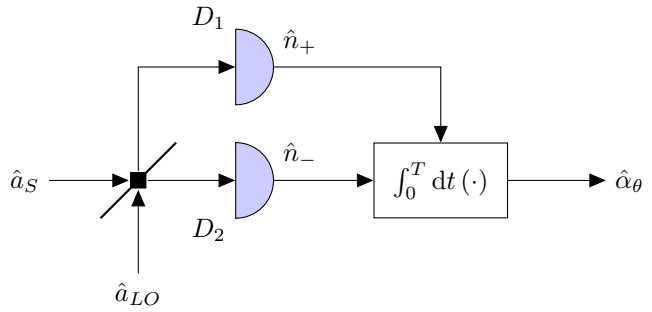


Figura 32 – Esquema de detecção homódina

incidentes E_+ e E_-, normalizado por $q/K = 1/2\sqrt{N_{LO}}$. Como desenvolvido na Apêndice A.3.4, o detector direto realiza a operação de medição do operador de número $\hat{n}$. Logo, denotamos o operador $\hat{\alpha}_\theta = \Delta\hat{n} = \hat{n}_+ - \hat{n}_-$, que é representado como função dos operadores de campo $\hat{a}_\pm$,

$$\hat{\alpha}_\theta = \frac{\hat{a}_+^\dagger \hat{a}_+ - \hat{a}_-^\dagger \hat{a}_-}{2\sqrt{N_{LO}}} \Longleftrightarrow \alpha_\theta = \frac{N_+ - N_-}{2\sqrt{N_{LO}}}. \tag{A.98}$$

em que a seta bilateral indica a equivalência estatística entre o operador e avariável aleatória clássica referente a medição desse operador, conforme apresentada na Equação (A.69). Logo,

$$\frac{\hat{a}_+^\dagger \hat{a}_+ - \hat{a}_-^\dagger \hat{a}_-}{2\sqrt{N_{LO}}} = \frac{\hat{a}_S^\dagger \hat{a}_{LO} + \hat{a}_{LO}^\dagger \hat{a}_S}{2\sqrt{N_{LO}}} = \frac{\mathrm{Re}\{\hat{a}_S \hat{a}_{LO}^\dagger\}}{\sqrt{N_{LO}}}. \tag{A.99}$$

Como o oscilador local está no estado $\left|\sqrt{N_{LO}}e^{j\theta}\right\rangle$, no limite $N_{LO} \to \infty$ podemos considerar[9] $\hat{a}_{LO}/\sqrt{N_{LO}} \to e^{j\theta}$ e $\hat{\alpha}_\theta \to \mathrm{Re}\{\hat{a}_s e^{-j\theta}\}$.

Dessa maneira, o esquema de medição apresentado na Figura 32 realiza a detecção da quadratura determinada pela fase relativa θ. Nos esquemas usuais, e utilizado comumente nos protocolos QKD com modulação gaussianda, o medidor homódino controla a fase do medidor homódino para escolher $\theta = 0$ ou $\theta = \pi/2$, em que o primeiro realiza a medição da parte real de $\hat{a}_S$ e o segundo, a parte imaginária. Por fim, para obter a função de probabilidade da medição de $\hat{\alpha}_\theta$, utilizamos a equivalência entre a FCC da variável aleatória que representa a medição do operador e a FCW do operador $\hat{\alpha}_\theta$, de modo que

$$M_{\alpha_\theta}(jv) = \left\langle e^{jv\alpha_\theta} \right\rangle = \left\langle e^{jv\hat{\alpha}_\theta} \right\rangle = \chi_W(\zeta^*, \zeta)\Big|_{\zeta = jve^{jv\theta/2}}. \tag{A.100}$$

Exemplo A.17 (Detecção homódina de um estado coerente)**.** *Sendo o sinal medido em um estado coerente $|\beta_\theta\rangle$ e sabendo que $\hat{a}_\theta \approx \mathrm{Re}\{\hat{a}_S e^{j\theta}\}$ no regime de alta potência do oscilador local e ainda que $\hat{a}_\theta |\beta_\theta\rangle = \beta_\theta |\beta_\theta\rangle$, a FCC é desenvolvida:*

$$\chi_W(\zeta^*, \zeta) = \chi_N(\zeta^*, \zeta)e^{-|\zeta|^2/2} = \langle\beta|e^{-\zeta\hat{a}_\theta^\dagger} e^{\zeta^*\hat{a}_\theta} e^{-|\zeta|^2/2}|\beta\rangle = e^{-\zeta\beta_\theta^*} e^{\zeta^*\beta_\theta} e^{-|\zeta|^2/2} \tag{A.101}$$

[9]Para um estado coerente, $\hat{a}_{LO}\left|\sqrt{N_{LO}}e^{j\theta}\right\rangle = \sqrt{N_{LO}}e^{j\theta}\left|\sqrt{N_{LO}}e^{j\theta}\right\rangle \to \frac{\hat{a}_{LO}}{\sqrt{N_{LO}}} = e^{j\theta}$

de modo que

$$\chi_W(\zeta^*,\zeta)\Big|_{\zeta=jve^{jv\theta/2}} = \exp\{jve^{j\theta/2}\beta_\theta - jve^{j\theta/2}\beta_\theta\}e^{v^2}. \tag{A.102}$$

A partir da FCW de $\hat{\alpha}_\theta$, a função densidade de probabilidade de α_θ condicionada ao estado inicial do sinal é obtida por meio da transformada inversa de Fourier:

$$p(\alpha_\theta|\,|\beta\rangle) = \mathcal{F}^{-1}\{M_{\alpha_\theta}(jv)\} = \frac{e^{-2(\alpha_\theta-\beta_\theta)^2}}{\sqrt{\pi/2}}. \tag{A.103}$$

Logo, α_θ é uma variável aleatória gaussiana com média β_θ e variância $1/4$, $\alpha_\theta \sim \mathcal{N}(\beta_\theta, 1/4)$.

Efeito da eficiência quântica não unitária.

Um dos detalhes importantes no modelo de detecção homódina é quando o fotodetector apresenta com eficiência quântica não unitária, isto é, quando apenas uma fração dos fótons incidentes no fotodetector são convertidos em uma fotocorrente. O modelo teórico utilizado para inserir o efeito da eficiência $\eta < 1$ é por meio de divisores de feixe *fictícios* de transmitância η antes de cada fotodetector ideal, em que a segunda porta de entrada é deixa em vazio, ou seja, em um estado de vácuo. Defina o operador de deslocamento $\hat{X}_\phi = \hat{a}^\dagger e^{i\phi} + \hat{a}e^{-i\phi}$ em que ϕ é a fase relativa entre o modo de entraa e o oscilador local, que é um estado coerente com amplitude $\beta = |\beta|e^{i\phi}$. Seja $\hat{u}$ e $\hat{v}$ os operadores dos modos de vácuo das entradas em vazio nos divisores de feixe fictícios e $\hat{n}_1$ e $\hat{n}_2$ os operadores de número relacionados às saídas dos fotodetectores. Então, a diferença de corrente na saída da detecção homódina Δi é proporcional ao valor esperado $\langle\hat{n}_1 - \hat{n}_2\rangle$ que, no limite do oscilador local de alta potência,

$$\Delta i = \lim_{|\beta|\to\infty} \frac{\langle\hat{n}_1 - \hat{n}_2\rangle}{\eta|\beta|} \tag{A.104}$$

$$= \langle\hat{X}_\phi\rangle + \sqrt{\frac{1-\eta}{\eta}}\left(\frac{\langle\hat{u}_\phi\rangle + \langle\hat{v}_\phi\rangle}{\sqrt{2}}\right). \tag{A.105}$$

Isso significa que a função de probabilidade de corrente de saída final é composta pela mistura de um componente de sinal de entrada, da quadratura $\hat{X}_\phi$ e a influência das quadraturas do estado de vácuo, $\hat{u}_\phi$ e $\hat{v}_\phi$. As componentes de vácuo tem distribuição normal $\mathcal{N}(0,(1- \ eta)/4\eta)$, e, para o modo de entrada em um estado coerente $|\alpha\rangle$, a distribuição $\hat{X}_\phi$ também é normal $\mathcal{N}(\alpha_i, 1/4)$. Então, $\Delta i \sim \mathcal{N}(\alpha_i, 1/4\eta)$.

Isso leva a um modelo mais simples para eficiência quântica não unitária BHD [126]. Como a influência de $\hat{u}$ e $\hat{v}$ na corrente de saída pode ser representada como um modo de vácuo único, é possível substituir os dois divisores de feixe fictícios por um único antes

de um dispositivo BHD de eficiência quântica unitária. Isso é de especial importância para contabilizar os efeitos da ineficiência de detecção no UD-CVQKD. A conversão de um modelo para outro ocorre da seguinte forma. A partir da diferença do operador numérico, $\hat{n}_1 - \hat{n}_2$, pode-se descartar todos os modos que não estão acoplados ao oscilador local (aqueles que irão desaparecer no limite LO forte) e definir o bosônico operador [10] $\hat{\Lambda} = (\hat{u} + \hat{v})/\sqrt{2}$, do qual segue que

$$\hat{n}_1 - \hat{n}_2 = \sqrt{\eta}\hat{b}(\sqrt{\eta}\hat{a}^\dagger + \sqrt{1-\eta}\hat{\Lambda}^\dagger) + \text{H. c.}, \tag{A.106}$$

onde H.c. representa o conjugado hermitiano. Desta expressão final, pode-se concluir que a diferença do operador numérico é equivalente, até um fator de $\sqrt{\eta}$, a uma medição de detecção homódina perfeita de modos interferidos por sinal/vácuo ($\hat{a}$ e $\hat{\Lambda}$). Esse arranjo é realizado adicionando-se um divisor de feixe fictício antes da eficiência da unidade BHD, o que leva às mesmas estatísticas de corrente de saída obtidas na Eq. (A.105).

Detecção Heteródina

A detecção heteródina parte do mesmo princípio da medição homódina, interferindo através de um *beam splitter* o sinal a ser medido com um oscilador local em regime de alta intensidade, mas utilizando o oscilador local deslocado para uma frequência intermediária em relação ao sinal. Essa manobra faz com que o fasor (semiclássico) ou o operador de aniquilação (quântico) surjam em componentes de fase diferentes do equivalente passa baixas e, pela projeção ortogonal, detectar ambas as qudadraturas do fasor ou operador de aniquilação.

Na análise do detector heteródino quântico, identicamente aos detectores direto e homódino, os operadores de campo e de aniquilação aparecem como a generalização direta da formulação apresentada. A frequência do oscilador local estará deslocada por ω_{IF} mas, diferentemente, será considerado juntamente com o modo do sinal, centrado na frequência ω um modo não excitado deslocado em frequência por $2\omega_{IF}$ na entrada do *beam splitter*, da seguinte maneira,

$$\hat{E}(x,y,t) = \frac{\hat{a}_s e^{-j\omega t}}{\sqrt{AT}} + \frac{\hat{a}_I e^{-j(\omega - 2\omega_{IF})t}}{\sqrt{AT}} \qquad \hat{E}_{LO}(x,y,t) = \frac{\hat{a}_{LO} e^{-j(\omega-\omega_{IF})t}}{\sqrt{AT}}, \tag{A.107}$$

onde I indica o campo de *imagem*. Sendo assim, o modo do sinal estará em uma frequência ω_{IF} acima do oscilador local e o modo de imagem estará na frequência ω_{IF} abaixo, o que resultará, pela interferência, batimentos de componentes desses modos na frequência intermediária.

[10] Observe que é um operador de aniquilação bosônico válido, pois preserva a relação de comutação canônica $[\hat{\Lambda}, \hat{\Lambda}^\dagger] = 1$.

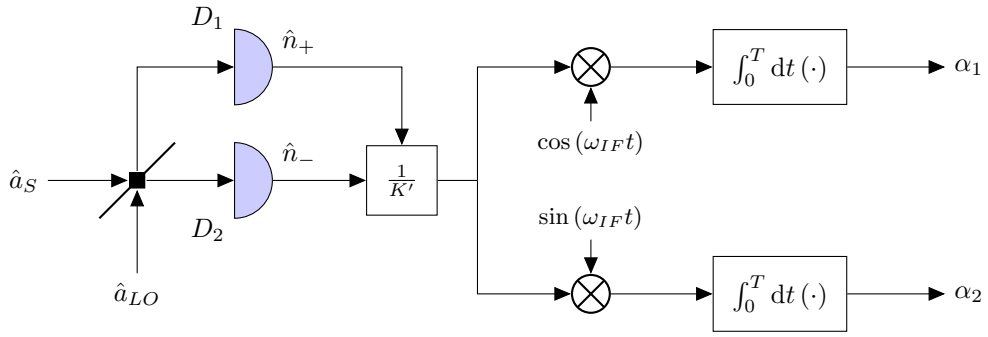


Figura 33 – Esquema do detector heteródino.

Segue que, realizando o mesmo procedimento da análise semiclássica do medidor heteródino, as fotocorrentes em cada braço de saída do *beam splitter* é obtida através dos operadores de campo

$$\hat{i}_\pm(t) = q\int_{\mathcal{A}} \mathrm{d}x\,\mathrm{d}y\,\hat{E}_\pm(x,y,t)^\dagger \hat{E}_\pm(x,y,t) \tag{A.108}$$

$$\begin{aligned} &= \frac{q}{2T}\Big(\hat{a}_S^\dagger\hat{a}_S + \hat{a}_I^\dagger\hat{a}_I + \hat{a}_{LO}^\dagger\hat{a}_{LO} + \mathrm{Re}\Big\{\hat{a}_S\hat{a}_I^\dagger e^{-j2\omega_{IF}t}\Big\} \\ &\qquad \pm \mathrm{Re}\Big\{\hat{a}_S\hat{a}_{LO}^\dagger e^{-j\omega_{IF}t}\Big\} \pm \mathrm{Re}\Big\{\hat{a}_I^\dagger\hat{a}_{LO}e^{-j\omega_{IF}t}\Big\}\Big) \end{aligned}, \tag{A.109}$$

levando à expressão para a diferença de correntes normalizada por k'

$$\frac{i_+(t) - i_-(t)}{k'} = \frac{2\,\mathrm{Re}\Big\{\hat{a}_S\hat{a}_{LO}^\dagger e^{-j\omega_{IF}t}\Big\} + 2\,\mathrm{Re}\Big\{\hat{a}_I^\dagger\hat{a}_{LO}e^{-j\omega_{IF}t}\Big\}}{T\sqrt{N_{LO}}} \tag{A.110}$$

.

Evidentemente, a manobra realizada leva os operadores de aniquilação dos sistemas do sinal, imagem e oscilador local às quadraturas da frequência intermediária. A saída de cada contador é então

$$\hat{\alpha}_1 = \frac{1}{k'}\int_0^T \mathrm{d}t\,(i_+(t) - i_-(t))\cos(\omega_{IF}t) \tag{A.111}$$

$$\hat{\alpha}_2 = \frac{1}{k'}\int_0^T \mathrm{d}t\,(i_+(t) - i_-(t))\sin(\omega_{IF}t) \tag{A.112}$$

$$\hat{\alpha} = \hat{\alpha}_1 + j\hat{\alpha}_2 = \frac{1}{k'}\int_0^T \mathrm{d}t\,(i_+(t) - i_-(t))e^{j\omega_{IF}t} \tag{A.113}$$

Para $\sqrt{N_{LO}} \to \infty$ e sabendo que os modos de entrada do divisor de feixe estão no sistema composto $\mathcal{H}_S \otimes \mathcal{H}_I$,

$$\hat{\alpha} = \lim_{N_{LO}\to\infty} \frac{1}{q\sqrt{N_{LO}}}\int_0^T \mathrm{d}t\,(i_+(t) - i_-(t))e^{j\omega_{IF}t} \tag{A.114}$$

$$= \lim_{N_{LO}\to\infty} \frac{\hat{a}_S\hat{a}_{LO}^\dagger + \hat{a}_I^\dagger\hat{a}_{LO}}{\sqrt{N_{LO}}} \tag{A.115}$$

$$= \hat{a}_S + \hat{a}_I \tag{A.116}$$

$$= \hat{a}_S \otimes \hat{I}_I + \hat{I}_S \otimes \hat{a}_I. \tag{A.117}$$

É possível notar que o operador referente à saída do medidor heteródino é idêntico ao operador da Equação (A.89), o qual comuta com seu conjugado e tem estatística de detecção idêntica à do operador de aniquilação do sistema principal. Logo, o esquema de detecção heteródina é a realização física do POVM de $\hat{a}_S$, realizando a medição de ambas as quadraturas do sinal medido. Resta que as variáveis aleatórias clássicas que representam as saídas do detector heteródino tem a mesma distribuição de probabilidades dos operadores $\hat{\alpha}_1$ e $\hat{\alpha}_2$, e considerando a equivalência entre $\hat{\alpha}$ e $\hat{a}_S$, é obtido que $\alpha \leftrightarrow \hat{a}_S$. Para o sistema do sinal em um estado coerente $|\beta\rangle$, a distribuição de probabilidades conjunta de detecção das quadraturas será gaussiana com valores médios β_1 e β_2 e variâncias $1/2$,

$$p(\alpha|\,|\beta\rangle = \frac{|\langle\alpha|\beta\rangle|^2}{\pi} = \frac{e^{-|\alpha-\beta|^2}}{\pi}. \tag{A.118}$$

Apêndice B

Tópicos em Teoria da Informação Clássica e Quântica

Nesta Seção serão abordados os tópicos básicos da teoria da informação, sendo definidas as quantidades de entropia, entropia relativa e informação mútua, que serão vistas como medidas razoáveis de informação e, a partir destas definições, será apresentado a capacidade de um canal de comunicação. Os conceitos abordados nesta seção foram formalizados matematicamente por Claude E. Shannon em seu trabalho intitulado "*A Mathematical Theory of Communication*" [71].

B.1 Teoria da informação Clássica

Começaremos pela definição de *entropia*, que informa a respeito da incerteza de uma variável aleatória. Seja X uma variável aleatória discreta com alfabeto $\mathcal{X}$ e função massa de probabilidade $p(x) = P[X = x], x \in \mathcal{X}$.

Definição B.1 (Entropia)**.** *A entropia de uma variável aleatória discreta* X *é definida como*

$$H(X) = -\sum_{x \in \mathcal{X}} p(x) log(p(x)). \tag{B.1}$$

É admitido que $0log(0) = 0$, justificado pelo fato de que o limite $xlog(x) \to 0$ na medida que x se aproxima de zero, e sendo mantida a continuidade. $H(X)$ pode também ser escrita como $H(p)$, uma vez que a entropia de uma variável aleatória é uma função de sua distribuição de probabilidades. A entropia de uma fonte com alfabeto $\mathcal{X} = \{0, 1\}$ e distribuição de probabilidade $P[X = 1] = p$ e $P[X = 0] = 1 - p$ apresenta maior incerteza quando os símbolos da fonte são distribuidos uniformemente.

A entropia também pode ser entendida como o valor esperado da variável aleatória $g(X) = log(\frac{1}{p(x)})$, onde $X \sim p(x)$. Logo,

$$H(X) = Elog\left(\frac{1}{p(x)}\right) \tag{B.2}$$

Para o caso de duas variáveis aleatórias conjuntamente distribuídas, sua entropia pode ser entendida como a entropia de um vetor aleatório.

Definição B.2 (Entropia conjunta)**.** *Para duas variáveis aleatórias* (X, Y) *com distribuição conjunta de probabilidades* $p(x, y)$*, a entropia conjunta é definida como*

$$\begin{aligned} H(X,Y) &= -\sum_{x\in\mathcal{X}}\sum_{y\in\mathcal{Y}} p(x,y) log\, p(x,y) && \text{(B.3)} \\ &= -E\, log\, p(X,Y) && \text{(B.4)} \end{aligned}$$

Também é definida a entropia de uma variável aleatória dada outra variável aleatória:

Definição B.3 (Entropia condicional)**.** *Para duas variáveis aleatórias* (X, Y) *com distribuição conjunta de probabilidades* $p(x, y)$*, a entropia condicional é definida como*

$$\begin{aligned} H(Y|X) &= \sum_{x\in\mathcal{X}} p(x) H(Y|X=x) && \text{(B.5)} \\ &= -\sum_{x\in\mathcal{X}} p(x) \sum_{y\in\mathcal{Y}} p(y|x) log(p(y|x)) && \text{(B.6)} \\ &= -\sum_{x\in\mathcal{X}}\sum_{y\in\mathcal{Y}} p(x,y) log(p(y|x)) && \text{(B.7)} \\ &= -E\, log\, p(Y|X) && \text{(B.8)} \end{aligned}$$

A entropia é uma medida de incerteza de uma variável aleatória baseada na sua distribuição de probabilidades, medindo a quantidade de informação necessária para representá-la. A entropia relativa é uma medida de distância entre duas distribuições de probabilidades.

Definição B.4 (Entropia Relativa)**.** *A entropia relativa, ou distância de* Kullback-Leibler *entre duas funções massa de probabilidade* $p_X(x) eq_X(x)$ *é definida como*

$$D(p||q) = \sum_{x\in\mathcal{X}} p_X(x) log\left(\frac{p(x)}{q(x)}\right) \tag{B.9}$$

A entropia relativa pode ser encarada como uma medida de ineficiência entre duas distribuições de probabilidades p e q. A informação mútua é uma medida de informação sobre o quanto uma variável aleatória diz sobre a outra.

Definição B.5 (Informação Mútua)**.** *Sejam duas variáveis aleatórias X e Y com distribuição conjunta de probabilidade $p(x, y)$ e distribuições marginais $p(x)$ e $p(y)$. A informação mútua é definida como a entropia relativa entre a distribuição conjunta e o produto as distribuições marinais:*

$$I(X;Y) = \sum_{x\in\mathcal{X}}\sum_{y\in\mathcal{Y}} p(x,y) log\left(\frac{p(x,y)}{p(x)p(y)}\right) \tag{B.10}$$

A Informação mútua informa qual a redução de incerteza sobre a variável X quando Y é conhecido, e vice-versa.

B.2 Teoria da Informação Quântica

Na teoria da informação clássica, a entropia é uma função da distribuição de probabilidade que rege a variável aleatória e que informa uma "quantidade de incerteza" da distribuição. Uma vez que a incerteza é conceito muito caro à teoria quântica, medidas entrópicas ocupam um lugar de ampla importância [4]. Nos sistemas quânticos, estados do sistema são "objetos probabilísticos", apresentando um tipo de distribuição de probabilidades através dos seus autovalores. Logo, a entropia de um sistema (que é uma medida de incerteza), é uma função do operador de densidade do sistema nos mesmos padrões da entropia de Shannon.

Definição B.6 (Entropia de Von Neuman)**.** *Seja $\hat{\rho}_A$ um estado do sistema quântico $\mathcal{H}_A$. A entropia $S(\hat{\rho}_A)$ do estado é definida como*

$$S(\hat{\rho}_A) = -\operatorname{tr}(\hat{\rho}_A \log \hat{\rho}_A). \tag{B.11}$$

Uma vez que os operadores de densidade implicam uma distribuição de probabilidades do estado do sistema, uma forte relação entre a entropia de Von Neuman e a entropia de Shannon é observada quando a primeira é calculada a partir da decomposição espectral do estado. Sejam λ_A autovalores e $|\lambda_A\rangle$ autovetores de $\hat{\rho}_A$ de modo que formam uma decomposição espectral do operador $\hat{\rho}_A = \sum_A \lambda_A |\lambda_A\rangle \langle\lambda_A|$, a entropia do estado quântico é dada por

$$S(\hat{\rho}_A) = -\sum_A \lambda_A \log \lambda_A = H(\lambda), \tag{B.12}$$

que é a entropia de Shannon dos autovalores[1] de $\hat{\rho}_A$. Considere uma variável aleatória X com alfabeto $\mathcal{X}$ e distribuição $p_X(x)$, e uma família (em inglês, *ensemble*) de estados puros

[1] Os autovalores de um operador de densidade correspondem a uma distribuição de probabilidade uma vez que $\lambda_i \leq 0$ para qualquer i e $\sum_i \lambda_i = 1$.

$\mathcal{E} = \{|\psi_x\rangle, p_X(x)\}$, $x \in \mathcal{X}$, que representa uma fonte de informação quântica que emite estados quânticos de acordo com a variável aleatória X. O estado da fonte é representado pelo operador de densidade $\hat{\rho} = \sum_{x\in\mathcal{X}} p_X(x)|\psi_x\rangle\langle\psi_x|$, que é uma mistura dos possívei estados emitidos pela fonte. A entropia $S(\hat{\rho})$ pode ser calculada pela obtenção dos autovalores de $\hat{\rho}$ ou, como será útil no caso de estados coerentes, pela matriz normalizada de Gramm.

Definição B.7 (Matriz de Gramm normalizada)**.** *Seja $\mathcal{E} = \{|\psi_i\rangle, p_i\}_{i=1}^n$ uma mistura de estados puros. A matriz de Gramm normalizada $\boldsymbol{G}$ tem elementos*

$$[\boldsymbol{G}]_{m,n} = \sqrt{p_m p_n}\,\langle\psi_m|\psi_n\rangle \tag{B.13}$$

que são os produtos interno dos estados $|\psi_m\rangle, |\psi_n\rangle \in \mathcal{E}$ normalizados pelas respectivas probabilidades.

O seguinte teorema assegura a igualdade entre as entropias de shannon dos autovalores $\hat{\rho}$ e de $\boldsymbol{G}$.

Teorema B.8 (Entropia da matriz de Gramm normalizada [127])**.** *Para uma mistura de estados puros $\mathcal{E} = \{|\psi_i\rangle, p_i\}_{i=1}^n$ de um sistema quântico de dimensão d, sendo $\hat{\sigma} = \sum_i p_i |\psi_i\rangle\langle\psi_i|$ o operador de densidade correspondente, temos que a matriz de Gramm $\boldsymbol{G}$ para $\mathcal{E}$ apresenta as seguintes propriedades:*

1. *$\boldsymbol{G}$ e $\hat{\sigma}$ tem os mesmos autovalores não negativos, inclusive as mesmas multiplicidades [128]. para o caso geral em que $n \neq d$, a diferença na quantidade de autovalores entre as matrizes $\hat{\sigma}$ e $\boldsymbol{G}$ é resolvida completando com autovalores nulos. Então, $\boldsymbol{G}$ e $\hat{\sigma}$ tem a mesma entropia de von Neumann, i.e., $S(\hat{\sigma}) = S(\boldsymbol{G})$.*
2. *$\boldsymbol{G}$ é uma matriz positiva e com trapo unitário. Ainda, se uma matriz arbitrária $m \times m$ $\boldsymbol{A}$ é positiva e tem $\mathrm{tr}(\boldsymbol{A}) = 1$, então $\boldsymbol{A}$ é a matriz de Gramm de uma mistura de m estados em um sistema de dimensão m.*

Entropia de estados gaussianos

Para o caso de estados quânticos gaussianos, é possível obter a entropia através da aplicação do teorema de Williamson diagonalizando a matriz de covariância do estado. O teorema de Williamson estabelece que toda matriz positiva de dimensão par pode ser diagonalizada pelo uso de transformações simpléticas. De maneira geral, uma transformação representada por uma matriz $\boldsymbol{S}$ é simplética se a seguinte condição for mantida

$$\boldsymbol{S}\Omega\boldsymbol{S}^T = \Omega. \tag{B.14}$$

sendo Ω a forma simplética da Equação (A.13). Dado um estado quântico gaussiano $\hat{\rho} \in \mathcal{D}(\mathcal{H}^{\otimes N})$ com matriz de covariância $\boldsymbol{V}$, de acordo com o teorema de Williamson, existe uma matriz simplética $\boldsymbol{S}$ tal que

$$\boldsymbol{\Sigma} = \boldsymbol{S}\boldsymbol{\Sigma}^{\oplus}\boldsymbol{S}^{T}, \qquad \boldsymbol{\Sigma}^{\oplus} = \bigoplus_{k=1}^{N} \nu_k \mathbf{I}, \tag{B.15}$$

onde ν_k são os autovalores simpléticos e $\Sigma^{\oplus}$ é a forma de Williamson de Σ, o espectro de autovalores simpléticos $\{\nu_k\}_{k=1}^{N}$ pode ser obtido a partir do módulo dos autovalores comuns da matriz simplética equivalente $\tilde{\boldsymbol{\Sigma}} = i\boldsymbol{\Omega}\boldsymbol{\Sigma}$ e correspondem às energias $\bar{n}_k = (\nu_k - 1)/2$ de N estados térmicos $\hat{\rho}^{th}(\bar{n}_1) \otimes \cdots \otimes \hat{\rho}^{th}(\bar{n}_N)$.

Então, sendo $\boldsymbol{S}$ a forma simplética correspondente a uma transformação unitária no espaço de Hilbert e a entropia sendo invariante a operações unitárias, segue que a entropia de Von Neumann $S(\hat{\rho})$ é exatamente a entropia do produto de N estados térmicos

$$S(\hat{\rho}) = \sum_{i=1}^{N} S(\hat{\rho}^{th}(\bar{n}_i)), \tag{B.16}$$

sendo a entropia de um estado térmico dada pela função entrópica bosônica

$$S(\hat{\rho}^{th}(\bar{n}_i)) = (\bar{n}_i + 1)\log(\bar{n}_i + 1) - \bar{n}_i \log \bar{n}_i \tag{B.17}$$

$$= \left(\frac{\nu_i + 1}{2}\right)\log\left(\frac{\nu_i + 1}{2}\right) - \left(\frac{\nu_i - 1}{2}\right)\log\left(\frac{\nu_i - 1}{2}\right). \tag{B.18}$$

Pela relação entre as entropias de Shannon e von Neumann, a entropia quântica herda algumas propriedades análogas, como a não negatividade ($S(\hat{\rho}) \geq 0$), nulidade para estados puros e limitada superiormente pelo logaritmo da dimensão do espaço, isto é, em um espaço de Hilbert $\mathcal{H}$ de dimensão d, temos que $S(\hat{\rho}) \leq \log(d)\, \forall\, \hat{\rho} \in \mathcal{D}(\mathcal{H})$, em que a igualdade é obtida para $\hat{\rho} = \hat{I}/d$, que é o estado maximamente misturado do sistema.

Propriedade B.9 (Concavidade)**.** *Seja $\hat{\rho} = \sum_x p_x \hat{\rho}_x$ uma mistura de estados quaisquer $\hat{\rho}_x \in \mathcal{D}(\mathcal{H})$ e p_x uma distribuição de probabilidades. Então, a entropia é côncava na mistura*

$$S(\hat{\rho}) \geq \sum_x p_x S(\hat{\rho}_x). \tag{B.19}$$

Em especial, se os estados $\hat{\rho}_i$ tem suporte em subespaços ortogonais, então a entropia da mistura $\hat{\rho}$ será dada por

$$S\left(\sum_i p_i \hat{\rho}_i\right) = H(p_i) + \sum_i p_i S(\hat{\rho}_i). \tag{B.20}$$

Propriedade B.10 (Invariância a isometrias)**.** *Seja $\hat{\rho} \in \mathcal{D}(\mathcal{H})$ e $\hat{U} : \mathcal{H} \to \mathcal{H}'$ uma isometria. A entropia de um estado é invariante a isometrias,*

$$S(\hat{\rho}) = S(\hat{U}\hat{\rho}\hat{U}^{\dagger}). \tag{B.21}$$

A entropia conjunta de um sistema composto AB é definida de modo análogo à entropia para um único modo.

Definição B.11 (Entropia Conjunta)**.** *A entropia conjunta $S(A, B)$ de um sistema composto AB é dada por*

$$S(\hat{\rho}_{AB}) = -\operatorname{tr}(\hat{\rho}_{AB} \log \hat{\rho}_{AB}), \tag{B.22}$$

$\hat{\rho}_{AB} \in \mathcal{D}(\mathcal{H}_A \otimes \mathcal{H}_B)$

Propriedade B.12 (Subaditividade da entropia de von Neumann)**.** *A entropia de um sistema composto AB é subaditiva*

$$S(\hat{\rho}_{AB}) \leq S(\hat{\rho}_A) + S(\hat{\rho}_B), \tag{B.23}$$

para todo estado $\hat{\rho}_{AB} \in \mathcal{D}(\mathcal{H}_A \otimes \mathcal{H}_B)$, sendo $\hat{\rho}_A = \operatorname{tr}_B(\hat{\rho}_{AB})$ e $\hat{\rho}_B = \operatorname{tr}_A(\hat{\rho}_{AB})$, e a igualdade é obtida quando $\hat{\rho}_{AB} = \hat{\rho}_A \otimes \hat{\rho}_B$, ou seja, é um estado separável.

No caso especial em que $\hat{\rho}_{AB}$ é um estado puro, temos que $S(\hat{\rho}_A) = S(\hat{\rho}_B)$. Uma importante classe de sistemas quânticos compostos são os estados clássicos-quânticos [113] em que, para uma mistura de estados quais quer, um sistema clássico é utilizado para funcionar como um tipo de registro de que estado quântico foi preparado e ajuda a aprender sobre a distribuição de p_i.

Definição B.13 (Estado Clássico-Quântico)**.** *O operador de densidade que corresponde a um conjunto clássico-quântico $\{p_i, |i\rangle \langle i| \otimes \hat{\rho}_i\}$ é dito um estado clássico-quântico e assume a seguinte forma*

$$\hat{\rho} = \sum_i p_i |i\rangle \langle i| \otimes \hat{\rho}_i. \tag{B.24}$$

A incerteza sobre este estado, que é uma mistura, se traduz na incerteza média dos estados pertencentes à mistura somada à incerteza da distribuição de probabilidades de p_x.

Teorema B.14 (Entropia do Sistema Clássico-Quântico)**.** *Estejam associados uma distribuição de probabilidades p_i, estados ortogonais $|i\rangle$ de um sistema de referência R e um conjunto de operadores de densidade $\hat{\rho}_i$ de um sistema A, de modo que formam a*

mistura $\sum_i p_i \left|i\right\rangle\!\left\langle i\right| \otimes \hat{\rho}_i \in \mathcal{D}(\mathcal{H}_R \otimes \mathcal{H}_A)$*, chamado de estado clássico quântico do sistema composto RA. Então, sua entropia será dada por*

$$S\left(\sum_i p_i \left|i\right\rangle \left\langle i\right| \otimes \hat{\rho}_i\right) = H(p_i) + \sum_i p_i S(\hat{\rho}_i). \tag{B.25}$$

Observamos que os resultados das Equações (B.20) e (B.25) são idênticos e que o estado clássico-quântico se torna semelhante à mistura considerada na Equação (B.20), cujo resultado é obtido para uma mistura de estados com suportes em subespaços ortogonais. Logo, o resultado da Equação (B.25) é obtido uma vez que os estados compostos $\left|i\right\rangle \left\langle i\right| \otimes \hat{\rho}_i$ possuem suportes ortogonais em $\mathcal{D}(\mathcal{H}_R \otimes \mathcal{H}_A)$.

Algumas relações da entropia de sistemas clássicos não são diretamente transferidas para os sistemas quânticos, sendo o caso de estados de sistemas conjuntos uma delas. Para o caso clássico, por exemplo, sejam X e Y duas variáveis aleatórias, a desigualdade $H(X) \leq H(X,Y)$ é sempre verdadeira, uma vez que a adição de um sistema pode apenas aumentar a incerteza sobre o sistema completo. No caso quântico, o sistema composto pode apresentar incerteza menor que a incerteza das partes. Por exemplo, considere o estado emaranhado de Bell $\left|\Psi^+\right\rangle_{AB} = (\left|00\right\rangle + \left|11\right\rangle)/\sqrt{2}$, que é um estado puro, logo $S(\left|\Psi^+\right\rangle) = 0$, e os estados nos sistemas isolados estão maximamente misturados e tem entropia $S(\mathrm{tr}_A(\left|\Psi^+\right\rangle\!\left\langle\Psi^+\right|)) = S(\mathrm{tr}_B(\left|\Psi^+\right\rangle\!\left\langle\Psi^+\right|)) = 1$.

Esse comportamento contraintuitivo com relação à entropia de sistemas clássicos pode ser interpretado operacionalmente a partir da definição da entropia condicional para estados quânticos.

Definição B.15 (Entropia quântica condicional)**.** *Seja* $\hat{\rho}_{AB} \in \mathcal{D}(\mathcal{H}_A \otimes \mathcal{H}_B)$*. A entropia quântica condicional* $S(\hat{\rho}_{AB}|B)$ *(ou apenas* $S(A|B)$*) é definida como a diferença entre a entropia conjunta* $S(\hat{\rho}_{AB})$ *e a entropia marginal* $S(B) = S(\hat{\rho}_B)$*,*

$$S(A|B) = S(A,B) - S(B). \tag{B.26}$$

Negatividade da Entropia Condicional

O exemplo apresentado com o estado de Bell mostra um comportamento estranho do ponto de vista clássico: a incerteza sobre um sistema composto pode ser menor do que sobre as partes. Isso implica que a entropia condicional na Definição B.15 pode ter valores negativos, o que é contraintuitivo e uma característica própria dos sistemas quânticos e está diretamente conectado a outra exclusividade quântica, o emaranhamento.

Uma interpretação operacional para a negatividade da entropia condicional pode ser obtida por meio do protocolo chamado de *state merging*. Digamos que Alice tem n cópias

de um estado bipartido $\hat{\rho}_{AB}$ e que os sistemas isolados são *qubits*. Alice quer então enviar todas as n cópias do sistema A para Bob por meio de um canal perfeito de *qubits* e ela tem acesso livre a um canal clássico lateral. Alice poderia, a princípio, fazer n usos do canal quântico para enviar os estados para Bob, mas é desejável que ela pudesse fazer menor número de usos do canal quântico possível. Se o estado $\hat{\rho}_{AB}$ tem entropia condicional positiva, então Alice pode realizar a tarefa de enviar os estados para Bob utilizando o canal quântico apenas aproximadamente $nS(A|B)$. Entretanto, se entropia condicional é negativa, Alice não precisa usar o canal quântico e, ao final do protocolo (*state merging*), Alice e Bob compartilham aproximadamente $-nS(A|B)$ *ebits*, que podem ser utilizados em outros protocolos de comunicação em que emaranhamento é um recurso consumido para execução de alguma tarefa.

Definição B.16 (Informação mútua quântica)**.** *A informação mútua quântica de um estado bipartido $\hat{\rho}_{AB} \in \mathcal{D}(\mathcal{H}_A \otimes \mathcal{H}_B)$ é definida por*

$$S(A:B) = S(A) + S(B) - S(A,B) \tag{B.27}$$

Assim como no caso clássico, a informação mútua quântica aceita as fatorações por meio da entropia condicional

$$S(A:B) = S(A) - S(A|B), \tag{B.28}$$
$$= S(B) - S(B|A), \tag{B.29}$$

tem um sentido de medida de correlações clássicas e quânticas entre os sistemas e é não negativa,

$$S(A:B) \geq 0. \tag{B.30}$$

As quantidades de informação até aqui apresentadas encontram, de alguma forma, suas respectivas contrapartes clássicas, mesmo que alguns resultados não sejam tão diretamente conectados (como é o caso da entropia condicional). Uma quantidade extremamente fundamental para a teoria da informação quântica e que não apresenta um paralelo na teoria da informação clássica é a *quantidade de informação acessível* de um sistema, limitada superiormente pelo conhecido *limitante de Holevo*. O limitante de Holevo configura uma das principais ferramentas da teoria da informação quântica para indicar a quantidade de informação que se pode obter ao observar um estado (ou sistema) quântico.

Para um pouco de contexto, criaremos um cenário onde dois protagonistas, Alice e Bob, tentam se comunicar a partir da transmissão de estados quânticos quando Alice, por

meio de um conjunto de índices $X = 1, \cdots n$ escolidos de acordo com uma distribuição de probabilidades clássica $p_1, \cdots, p_n$, envia para Bob um estado $\hat{\rho}_X$ escolhido do conjunto $\hat{\rho}_1, \cdots, \hat{\rho}_n$. Bob, através de medições dos estados recebidos, tenta estimar qual estado foi enviado, tendo como resultado uma variável aleatória Y.

O objetivo então é que Bob escolha um conjunto de operadores de medição que maximize a informação mútua $I(X;Y)$. A informação acessível é então a máxima informação mútua $I(X;Y)$ obtida considerando todos os conjuntos de medição possíveis.

Teorema B.17 (Limitante de Holevo)**.** *Seja $\hat{\rho}_x$ um estado preparado por Alice, onde $X = 0, 1, \cdots, n$ com probabilidades $p_0, p_1, \cdots, p_n$. Bob realiza medições descritas por POVM's $\{E_y\} = \{E_0, E_1, \cdots, E_m\}$ no estado $\hat{\rho}_x$, indicando um resultado de medição Y. O limitante de Holevo indica que para qualquer medição realizada, Bob obterá*

$$I(X;Y) \leq S\left(\sum_x p_x \hat{\rho}_x\right) - \sum_x p_x S(\hat{\rho}_x) \tag{B.31}$$

O limitante de Holevo é uma quantidade importante da teoria da informação quântica, sendo conhecida também como a quantidade de Holevo χ. Uma das consequências diretas do limitante de Holevo é que nenhum procedimento na mecânica quântica consegue distinguir dois estados quânticos não ortogonais de maneira indubitável. Ocorre que, pela concavidade da entropia de Von Neumann, a generalização da Equação (B.20) para estados quaisquer (não necessariamente com suportes em subespaços orotgonais) se torna uma desigualdade

$$S\left(\sum_i p_i \hat{\rho}_i\right) \leq H(p_i) + \sum_i p_i S(\hat{\rho}_i), \tag{B.32}$$

o que permite estabelecer o seguinte intervalo:

$$I(X;Y) \leq S\left(\sum_i p_i \hat{\rho}_i\right) - \sum_i p_i S(\hat{\rho}_i) \leq H(X). \tag{B.33}$$

A Equação (B.33) estabelece que o limitante de Holevo, que é a diferença entre a incerteza sobre a mistura dos possíveis estados da fonte e a incerteza média dos estados da fonte, se localiaza entre a informação mútua entre os a variável aleatória X que indica quais estados foram enviados de Alice para Bob e a variável aleatória Y indicando os resultados das medições efetuadas por Bob, e a incerteza sobre qual estado foi transmitido.

Desta forma, com a utilização de estados quânticos para enviar alguma informação entre duas partes, o uso de dois estados quânticos não ortogonais escolhidos de acordo

com uma distribuição de probabilidades, a informação acessível será estritamente menor que a entropia da distribuição de probabilidades. No contexto das comunicações clássicas, não há razão para que o mesmo resultado seja observado quando transmitidos dois sinais de acordo com uma distribuição de probabilidades. A única aproximação do resultado da mecânica quântica possível é os símbolos sejam transmitidos de acordo com duas distribuições de probabilidade $\{p, 1-p\}$ e $\{q, 1-q\}$.

É possível obter uma versão quântica da entropia relativa, a qual se mostra extremamente útil no desenvolvimento de diversos resultados da informação quântica.

Definição B.18 (Entropia Relativa Quântica)**.** *Seja A um sistema quântico e $\hat{\rho}, \hat{\sigma} \in \mathcal{D}(\mathcal{H}_A)$. A entropia relativa do estado $\hat{\rho}$ para $\hat{\sigma}$ é definida como*

$$S(\hat{\rho}||\hat{\sigma}) = \mathrm{tr}(\hat{\rho}\log\hat{\rho}) - \mathrm{tr}(\hat{\rho}\log\hat{\sigma}). \tag{B.34}$$

Na Equação (B.34), para que $S(\hat{\rho}||\hat{\sigma})$ assuma valores finitos, é preciso que o suporte de $\hat{\rho}$ esteja contido no suporte de $\hat{\sigma}$. Caso essa condição não seja respeitada, o suporte de $\hat{\rho}$ terá interseção não trivial com o núcleo de $\hat{\sigma}$, implicando na não separabilidade dos estados. A Entropia relativa parece indicar uma medida de distância entre os estados, não sendo devido ao fato de que não há simetria em $S(\hat{\rho}||\hat{\sigma})$ e a desigualdade triangular não é obedecida. Um propriedade da entropia relativa é sua não negatividade, conhecida como desigualdade de Klein, definida a seguir.

Teorema B.19 (Desigualdade de Klein)**.** *Sejam $\hat{\rho}$ e $\hat{\sigma}$ estados quânticos, a entropia relativa $S(\hat{\rho}||\hat{\sigma})$ é não negativa,*

$$S(\hat{\rho}||\hat{\sigma}) \geq 0, \tag{B.35}$$

com igualdade apenas se $\hat{\rho} = \hat{\sigma}$.

Extremalidade de Estados Gaussianos

Aprofundando no tema do estados Gaussianos, uma das suas principais características (e das mais relevantes para a teoria da informação) é que eles são "extremos" para funcionais contínuos, aditivos e inveriantes a operações unitárias locais. O seguinte conceito é necessário.

Definição B.20 (Estado Gaussiano Equivalente)**.** *Seja $\hat{\sigma}$ um estado quântico qualquer com primeiro e segundo momentos estatísticos finitos $\boldsymbol{r}(\hat{\sigma})$ e $\boldsymbol{\Gamma}(\hat{\sigma})$ respectivamente. Então, o estado gaussiano $\hat{\sigma}^G$ em que $\boldsymbol{r}(\hat{\sigma}^G) = \boldsymbol{r}(\hat{\sigma})$ e $\boldsymbol{\Gamma}(\hat{\sigma}^G) = \boldsymbol{\Gamma}(\hat{\sigma})$ é chamado de estado gaussiano equivalente.*

Para a entropia de von Neumann, tem-se que $S(\hat{\sigma}^G) \geq S(\hat{\sigma})$, que pode ser desenvolvido da seguinte forma [103]:

$$S(\hat{\sigma}^G) - S(\hat{\sigma}) = \mathrm{tr}[\hat{\sigma}(\ln\hat{\sigma} - \ln\hat{\sigma}^G)] + \mathrm{tr}[(\hat{\sigma} - \hat{\sigma}^G)\ln\hat{\sigma}^G], \tag{B.36}$$

em que o primeiro termo do lado direito da igualdade é a entropia relativa, a qual é não negativa, e o segundo termo é nulo por conta de $\hat{\sigma}$ e $\hat{\sigma}^G$ tem os mesmos primeiro e segundo momentos e $\ln\hat{\sigma}^G$ é um polinômio de segunda ordem nos operadore bosonicos. Essa propriedade da entropia dos estados gaussianos é generalizada no seguinte teorema

Teorema B.21 (Extremalidade dos Estados Gaussianos [23])**.** *Seja $f : \mathcal{B}(\mathcal{H}^{\otimes\mathcal{N}}) \to \mathbb{R}$ um funcional contínuo, fortemente superaditivo e invariante a operações unitárias locais. Então, para qualquer operador de densidade σ com primeiro e segundo momentos finitos, tem-se que*

$$f(\hat{\sigma}) \geq f(\hat{\sigma}^G). \tag{B.37}$$

Teorema B.22 (Produto de Hilbert-Schmidt de Estados Gaussianos)**.** *Para dois estados gaussianos arbitrários de n modos $\hat{\rho}_1$ e $\hat{\rho}_2$ com matrizes de covariância $\mathbf{\Sigma}_1$ e $\mathbf{\Sigma}_2$ e vetores de deslocamento $\boldsymbol{r}_1$ e $\boldsymbol{r}_2$, respectivamente, o produto interno (ou a sopreposição) entre $\hat{\rho}_1$ e $\hat{\rho}_2$ é dado por*

$$\mathrm{tr}(\hat{\rho}_1\hat{\rho}_2) = \frac{2^n}{\sqrt{\det(\mathbf{\Sigma}_1 + \mathbf{\Sigma}_2)}} e^{-(\boldsymbol{r}_1-\boldsymbol{r}_2)^T(\mathbf{\Sigma}_1+\mathbf{\Sigma}_2)^{-1}(\boldsymbol{r}_1-\boldsymbol{r}_2)}. \tag{B.38}$$

B.3 Noções de Distância na Informação Quântica

O conceito de uma medida de distância entre distribuições de probabilidade detêm um papel de extrema importância na teoria da informação clássica. A própria noção de informação mútua entre duas variáveis aleatórias é obtida da divergência de Kullback-Leibler, uma medida de entropia. Uma vez que estados quânticos possuem, de forma natural, uma descrição intrinsecamente aleatória, a noção de distância entre dois estados quânticos aparece com certa naturalidade. A preservação de informação quântica submetida a um processo pode ser dada a partir de medidas estáticas, informando a similaridade (ou proximidade) entre dois estados quânticos, ou medidas dinâmicas, revelando o quanto a informação tem sido preservada durante um processo dinâmico, utilizando medidas estáticas no seu desenvolvimento [2].

Nesta seção apresentaremos duas medidas fundamentais de distância entre estados quânticos que além de estarem intimamente relacionadas, possuem um papel operacional

importante. Antes de explorar as noções de distância entre estados quânticos, faremos um breve comentário sobre norma de operadores lineares.

---

p-Normas de Schatten [129]

Uma norma no espaço de operadores lineares em espaços de Hilbert $\mathcal{L}(\mathcal{H}_X, \mathcal{H}_Y)$ é uma função $\|\cdot\|$ que satisfaz às seguintes propriedades:

1. Positividade semidefinida: $\|\hat{A}\| \geq 0$ para todo $\hat{A} \in \mathcal{L}(\mathcal{H}_X, \mathcal{H}_Y)$, sendo $\|\hat{A}\| = 0$ *s.s.s.* $\hat{A} = \hat{0}$.
2. Escalabilidade positiva: $\|\alpha\hat{A}\| = |\alpha|\|\hat{A}\|$ para todo $\hat{A} \in \mathcal{L}(\mathcal{H}_X, \mathcal{H}_Y)$ e $\alpha \in \mathbb{C}$.
3. Desigualdade triangular: $\|A \hat{+} \hat{B}\| \leq \|\hat{A}\| + \|\hat{B}\|$ para todo $\hat{A}, \hat{B} \in \mathcal{L}(\mathcal{H}_X, \mathcal{H}_Y)$.

Dentre as possíveis normas no espaço dos operadores lineares, a família de p-normas de Schatten (*Schatten p-norms*) inclui as normas mais utilizadas na teoria da informação quântica, das quais destacaremos a norma de Frobenius e a norma do traço. Uma p-norma de Schatten, para qualquer $p \geq 1$ real, é dada por

$$\|\hat{A}\|_p = \left(\mathrm{tr}[(\hat{A}^\dagger \hat{A})^{\frac{p}{2}}]\right)^{\frac{1}{p}}, \tag{B.39}$$

para qualquer operador $\hat{A} \in \mathcal{L}(\mathcal{H}_X, \mathcal{H}_Y)$ e, no limite $p \to \infty$,

$$\|\hat{A}\|_\infty = \max_{\substack{u \in \mathcal{H}_X, \\ ||u|| \leq 1}} ||\hat{A}u||. \tag{B.40}$$

A 1-norma de Schatten é chamada de *norma do traço*, de modo que

$$\|\hat{A}\|_1 = \mathrm{tr}(\sqrt{\hat{A}^\dagger \hat{A}}) = \mathrm{tr}\,|\hat{A}|\,, \tag{B.41}$$

que é igual à soma dos valores singulares de $\hat{A}$, sendo $|\hat{A}| = \sqrt{\hat{A}^\dagger \hat{A}}$. Para $p = 2$, temos que a 2-norma de Schatten é chamada de *norma de Frobenius*,

$$\|\hat{A}\|_2 = \sqrt{\mathrm{tr}(\hat{A}^\dagger \hat{A})} = \sqrt{(\hat{A}^\dagger, \hat{A})} \tag{B.42}$$

sendo $(\hat{A}^\dagger, \hat{A})$ o produto interno de Hilbert-Schmidt para operadores lineares e $\|\cdot\|_2$ é a generalização da norma euclidiana entre vetores para operadores em $\mathcal{L}(\mathcal{H}_X, \mathcal{H}_Y)$.

A primeira medida de distância entre estados quânticos que apresentamos é a distância do traço, definida a seguir.

Definição B.23 (Distância do Traço)**.** *A distância do traço entre dois estados quânticos* $\hat{\rho}$, $\hat{\sigma} \in \mathcal{D}(\mathcal{H})$ *é dada pela norma do traço da diferença,*

$$\|\hat{\rho} - \hat{\sigma}\|_1 = tr|\hat{\rho} - \hat{\sigma}|. \tag{B.43}$$

A distância do traço entre estados quânticos definida a partir da norma do traço tem os seguintes limitantes

$$0 \leq \|\hat{\rho} - \hat{\sigma}\|_1 \leq 2, \tag{B.44}$$

uma vez que a norma do traço é não negativa e igual a zero *s.s.s.* $\hat{\rho} = \hat{\sigma}$ e, pela desigualdade triangular, $\|\hat{\rho} - \hat{\sigma}\|_1 \leq \|\hat{\rho}\|_1 + \|\hat{\sigma}\|_1 = 2$. Logo, em muitos casos é útil a definição da distância do traço normalizada

$$D(\hat{\rho}, \hat{\sigma}) = \frac{1}{2}\|\hat{\rho} - \hat{\sigma}\|_1. \tag{B.45}$$

Uma maneira interessante de interpretar a distância do traço é utilizando a representação dos estado na esfera de Bloch de modo que, para $\vec{r}$ e $\vec{s}$ sendo os vetores de Bloch dos estados $\hat{\rho}$, $\hat{\sigma} \in \mathcal{D}(\mathbb{C}^2)$, respectivamente, então

$$D(\hat{\rho}, \hat{\sigma}) = \frac{1}{2}tr|\hat{\rho} - \hat{\sigma}| = \frac{|\vec{r} - \vec{s}|}{2}, \tag{B.46}$$

e a distância do traço entre os estados é exatamente a metade da distância euclidiana entre seus vetores na esfera de Bloch, levando a uma interessante interpretação geométrica. Entretanto,

As interpretações mais importantes para a distância do traço entre estados quânticos se relacionam com as probabilidades de detecção e distinguibilidade de estados. O primeiro resultado relaciona a distância do traço com a maior diferença em probabilidade de dois estados $\hat{\rho}$, $\hat{\sigma} \in \mathcal{D}(\mathcal{H})$ terem o mesmo resultado de medição,

$$\frac{1}{2}\|\hat{\rho} - \hat{\sigma}\|_1 = \max_{\hat{0} \leq \hat{P} \leq \hat{I}} tr(\hat{P}(\hat{\rho} - \hat{\sigma})), \tag{B.47}$$

sendo a maximização sobre todos os projetores $\hat{P} \in \mathcal{L}(\mathcal{H})$. O resultado para um único projeto pode ser derivado para um POVM.

Teorema B.24. *Seja* $\left\{\hat{\Lambda}_m\right\}$ *um POVM,* $\hat{\rho}$, $\hat{\sigma} \in \mathcal{D}(\mathcal{H})$ *e defina* $p_m = \mathrm{tr}(\hat{\Lambda}_m\rho)$ *e* $q_m = \mathrm{tr}(\hat{\Lambda}_m\sigma)$ *as probabilidades de obter uma saída* m*. Então*

$$||\hat{\rho} - \hat{\sigma}||_1 = \max_{\left\{\hat{\Lambda}_m\right\}} \sum_m |p_m - q_m|, \tag{B.48}$$

sendo a maximização sobre todos os POVM's $\left\{\hat{\Lambda}_m\right\}$ *e o somatório no lado esquerdo da igualdade é um termo proporcional*[2] *à norma do traço para distribuições de probabilidade.*

[2]A norma do traço para duas distribuições de probabilidade $\{p_x\}$ e $\{q_x\}$ é $D(p_x, q_x) = \frac{1}{2}\sum_x |p_x - q_x|$.

Então, a distância do traço indica que dois estados quânticos são tão distantes quanto a maior distância (do traço) entre as distribuições de probabilidades resultantes de medições realizadas por algum POVM. Ou ainda, a distância do traço é um limitante superior alcançável para a distância do traço entre distribuições de probabilidade resultantes de medições realizadas nos estados quânticos, levando à seguinte interpretação operacional.

Interpretação operacional para a distância do traço.
A distância do traço entre dois estados é uma medida de distinguibilidade. Suponha que Bob prepara dois estados quânticos $\hat{\rho}_0$ e $\hat{\rho}_1$ com mesma probabilidade, cuja escolha é representada pela variável aleatória X com distribuição $p_X(0) = p_X(1) = 1/2$. Alice irá tentar distinguir entre os estados realizando um POVM com elementos $\hat{\Lambda} = \left\{\hat{\Lambda}_0, \hat{\Lambda}_1\right\}$, em que os índices indicam os respectivos estados preparados por Bob. Defina Y como sendo a variável aleatória indicando a saída do POVM e $p_{suc}(\hat{\Lambda})$ a probabilidade de sucesso em detectar corretamente o estado preparado por Bob. Então,

$$p_{suc}(\hat{\Lambda}) = p_{Y|X}(0|0) + p_{Y|X}(1|1) = \mathrm{tr}(\hat{\Lambda}_0\hat{\rho}_0)\frac{1}{2} + \mathrm{tr}(\hat{\Lambda}_1\hat{\rho}_1)\frac{1}{2}, \tag{B.49}$$

que, utilizando a relação de completude do POVM, $\Lambda_0 + \Lambda_1 = \hat{I}$,

$$p_{suc}(\hat{\Lambda}) = \frac{1}{2}\Big[\mathrm{tr}(\hat{\Lambda}_0\hat{\rho}_0) + \mathrm{tr}((\hat{I} - \Lambda_0)\hat{\rho}_1)\Big] \tag{B.50}$$

$$= \frac{1}{2}\Big[1 + \mathrm{tr}(\hat{\Lambda}_0(\hat{\rho}_0 - \hat{\rho}_1))\Big]. \tag{B.51}$$

Como Alice tem liberdade na escolha do POVM para distinguir entre $\hat{\rho}_0$ e $\hat{\rho}_1$, a maior probabilidade de sucesso p_{suc} de distinguir entre dois estados quânticos é uma maximização sobre os POVMs de modo que

$$p_{suc} = \max_{\{\hat{\Lambda}\}} p_{suc}(\hat{\Lambda}) = \frac{1}{2}\left(1 + \max_{\{\hat{\Lambda}\}} \mathrm{tr}[\hat{\Lambda}_0(\hat{\rho}_0 - \hat{\rho}_1)]\right) \tag{B.52}$$

$$= \frac{1}{2}\left(1 + \frac{1}{2}\|\hat{\rho}_0 - \hat{\rho}_1\|_1\right). \tag{B.53}$$

Logo, dois estados são indistinguíveis quando $\|\hat{\rho}_0 - \hat{\rho}_1\|_1 = 0$ e podem ser perfeitamente distinguíveis quando $\|\hat{\rho}_0 - \hat{\rho}_1\|_1$ é máximo e então a distância do traço é linearmente relacionada à máxima probabilidade de distinguir entre dois estados quânticos. O caso inverso pode então ser facilmente obtido, definindo $p_e = 1 - p_{suc}$ como a menor probabilidade de erro em distinguir dois estados e é conhecido como o limitante de Helstrom [130],

$$p_e = \frac{1}{2}\left(1 - \frac{1}{2}\|\hat{\rho}_0 - \hat{\rho}_1\|_1\right). \tag{B.54}$$

Das diversas propriedades da distância do traço, destacaremos a contração para operações preservadoras do traço (ou monotonicidade) e a convexidade da segunda entrada.

Propriedade B.25 (Monotonicidade da distância do traço)**.** *Seja $\mathcal{N}_{A\to B} \in \mathcal{Q}(\mathcal{H}_A \to \mathcal{H}_B)$ um canal quântico e $\hat{\rho}$, $\hat{\sigma} \in \mathcal{D}(\mathcal{H})$. Então, a distância do traço é monotônica com relação à ação do canal $\mathcal{N}_{A\to B}$:*

$$\|\mathcal{N}(\hat{\rho}) - \mathcal{N}(\hat{\sigma})\|_1 \leq \|\hat{\rho} - \hat{\sigma}\|_1. \tag{B.55}$$

Operacionalmente, significa que nenhuma operação CPTP pode tornar dois estados mais distinguíveis. Em especial, sendo a operação de traço parcial um tipo de *canal de descarte*, sendo $\hat{\rho}$ e $\hat{\sigma}$ estados de um sistema composto, observar apenas parte do sistema não ajuda na distinção entre os estados.

Propriedade B.26 (Convexidade do Traço)**.** *A distância do Traço é convexa na primeira entrada.*

$$D\left(\sum_i p_i\hat{\rho}_i, \hat{\sigma}\right) \leq \sum_i p_i D(\hat{\rho}_i, \hat{\sigma}), \tag{B.56}$$

em que p_i é uma distribuição de probabilidades. Por simetria, também é convexa na segunda entrada.

Ainda, motivado pela interpretação operacional da distância do traço na distinguibilidade entre estados quânticos, naturalmente é possível estender o conceito de distinguibilidade para a noção de distância entre canais quânticos. Ou seja, é possível definir uma noção de distância entre canais quânticos imbuída de sentido operacional? Par tal, é possível derivar uma formulação análoga à distinção entre estados quânticos com o teste de hipóteses e aplicá-la aos canais.

Suponha que Alice e Bob irão realizar uma tentativa de discriminação entre canas quânticos da seguinte maneira. (i) Alice prepara um estado $\hat{\rho}_A$ e o envia para Bob. (ii) Bob escolhe entre dois canais quânticos, $\mathcal{M}, \mathcal{N} \in \mathcal{Q}(\mathcal{H}_A \to \mathcal{H}_B)$, de modo equiprovável para atuar em $\hat{\rho}_A$ e envia a saída do canal de volta para Alice. (iii) Alice realiza alguma medição para tentar distinguir estimar qual canal foi utilizado por Bob. A tarefa que Alice deve realizar é a de distinguir entre os estados $\mathcal{M}(\hat{\rho}_A)$ e $\mathcal{N}(\hat{\rho}_A)$ e a maior probabilidade de acerto é dada pela Equação (B.53). Contudo, Alice tem liberdade na escolha de $\hat{\rho}_A$ e pode escolher o estado que maximiza a distância do traço.

Contudo, afim de conceder a Alice total liberdade na manipulação dos seus sistemas, é possível considerar que ela prepara um estado de um sistema composto $\hat{\rho}_{R_n A} \in \mathcal{D}(\mathcal{H}_{R_n} \otimes \mathcal{H}_A)$, sendo R um sistema de referência com dimensão n tão grande quanto necessária, mantém o sistema R e envia o sistema A para Bob. Então, a maior probabilidade de sucesso de distinguir entre os canais quânticos é obtido por

$$\frac{1}{2}\left(1 + \frac{1}{2}\sup_{n}\max_{\hat{\rho}_{R_n A}} \|(\mathcal{I}_{R_n} \otimes \mathcal{M})(\hat{\rho}_{R_n A}) - (\mathcal{I}_{R_n} \otimes \mathcal{N})(\hat{\rho}_{R_n A})\|_1\right), \tag{B.57}$$

e a medida de distância resultante é definida como a norma do diamante entre canais.

Definição B.27 (Norma do diamante)**.** *Sejam $\mathcal{M}, \mathcal{N} \in \mathcal{Q}(\mathcal{H}_A \to \mathcal{H}_B)$ canais quânticos, a norma do diamante é definida como*

$$\|\mathcal{M} - \mathcal{N}\|_\diamondsuit = \sup_{n}\max_{\hat{\rho}_{R_n A}} \|(\mathcal{I}_{R_n} \otimes \mathcal{M})(\hat{\rho}_{R_n A}) - (\mathcal{I}_{R_n} \otimes \mathcal{N})(\hat{\rho}_{R_n A})\|_1, \tag{B.58}$$

em que $\hat{\rho}_{R_n A} \in \mathcal{D}(\mathcal{H}_{R_n} \otimes \mathcal{H}_A)$.

A segunda medida apresentada, que na verdade é uma *pseudo-métrica*, é a Fidelidade entre dois estados quânticos. Apesar de não possuir características tão intuitivas a princípio, pode ser utilizada para avaliar a evolução de estados quânticos submetidos a algum processo ou servir de base para definição de uma distância entre estados.

Definição B.28 (Fidelidade Quântica)**.** *Sejam $\hat{\rho}$ e $\hat{\sigma}$ dois estados quânticos quaisquer. A fidelidade $F(\hat{\rho}, \hat{\sigma})$ é definida como*

$$F(\hat{\rho}, \hat{\sigma}) = tr\sqrt{\hat{\rho}^{\frac{1}{2}}\hat{\sigma}\hat{\rho}^{\frac{1}{2}}}. \tag{B.59}$$

Uma característica interessante da fidelidade é que, para um estado puro $|\psi\rangle$ e um segundo estado $\hat{\rho}$ arbitrário, temos que $F(|\psi, \hat{\rho}\rangle) = \sqrt{\langle\psi|\hat{\rho}|\psi\rangle}$. Entretanto, algumas propriedades podem ser melhor desenvolvidas a partir do teorema de Uhlmann que, mesmo não provendo uma maneira mais simples para calcular a fidelidade, serve como uma ferramenta teórica útil.

Teorema B.29 (Teorema de Uhlmann)**.** *Sejam ρ e σ estados quânticos de um sistema Q. Um segundo sistema quântico, R, é preparado de forma idêntica a Q. Então,*

$$F(\hat{\rho}, \hat{\sigma}) = \max_{|\psi\rangle, |\varphi\rangle} |\langle\psi|\varphi\rangle| \tag{B.60}$$

onde a maximização é sobre todas as purificações $|\psi\rangle$ e $|\varphi\rangle$ de ρ e σ, respectivamente, no sistema RQ.

Utilizando o teorema de Uhlmann, é possível ver rapidamente que a fidelidade é simétrica nas suas entradas e que $0, \leq F(\hat{\rho}, \hat{\sigma}) \leq 1$, de modo que a fidelidade é máxima quando $\hat{\rho} = \hat{\sigma}$ e nula se $\hat{\rho}$ e $\hat{\sigma}$ tem suportes ortogonais, implicando na possibilidade de distinguibilidade perfeita entre os estados.

Ainda, é possível obter algumas propriedades da fidelidade análogas às da norma do traço, como a monotonicidade sob operações preservadoras do traço, $F(\mathcal{E}(\hat{\rho}), \mathcal{E}(\hat{\sigma})) \geq F(\hat{\rho}, \hat{\sigma}))$ e a concavidade forte.

Teorema B.30 (Concavidade forte da Fidelidade)**.** *Sejam* $\{\hat{\rho}_i, p_i\}$ *e* $\{\hat{\sigma}_i, q_i\}$ *conjuntos de estados quânticos de modo que* $\sum_i p_i = \sum_i q_i = 1$*. Então,*

$$F(\sum_i p_i \hat{\rho}_i, \sum_i q_i \hat{\sigma}_i) \geq \sum_i \sqrt{p_i q_i} F(\hat{\rho}_i, \hat{\sigma}_i). \tag{B.61}$$

Outras propriedades para a fidelidade é que ela fornece expressões para limitantes inferiores e superiores para a norma do traço,

$$1 - F(\hat{\rho}, \hat{\sigma}) \leq \frac{1}{2} \|\hat{\rho} - \hat{\sigma}\|_1 \leq \sqrt{1 - F^2(\hat{\rho}, \hat{\sigma})}, \tag{B.62}$$

e que, para estados gaussianos de um modo, pode ser calculada diretamente dos momentos estatísticos que os descrevem:

Definição B.31 (Fidelidade para Estados Gaussianos)**.** *A fidelidade entre dois estados gaussianos de um modo* $\hat{\rho}_0(\bar{\boldsymbol{x}}_0, \boldsymbol{V}_0)$ *e* $\hat{\rho}_1(\bar{\boldsymbol{x}}_1, \boldsymbol{V}_1)$ *é dada por*

$$F(\hat{\rho}_0, \hat{\rho}_1) = \sqrt{\frac{2}{\sqrt{\Delta + \delta} - \sqrt{\delta}} \exp\left\{ -\frac{1}{2} \boldsymbol{d}^T (\boldsymbol{V_0} - \boldsymbol{V_1})^{-1} \boldsymbol{d} \right\}}, \tag{B.63}$$

em que $\Delta = \det(\boldsymbol{V_0} + \boldsymbol{V_1})$*,* $\delta = (\det \boldsymbol{V_0} - 1)(\det \boldsymbol{V_1} - 1)$ *e* $\boldsymbol{d} = \boldsymbol{x_1} - \boldsymbol{x_0}$*.*