



Universidade Federal de Campina Grande
Centro de Engenharia Elétrica e Informática
Programa de Pós-Graduação em Engenharia Elétrica

Tese de Doutorado

**Mapas de Shannon-Kotel'nikov na
Distribuição Quântica de Chaves com
Variáveis Contínuas**

Edmar José do Nascimento

Francisco Marcos de Assis

Orientador

Campina Grande – PB

Abril - 2017

Universidade Federal de Campina Grande
Centro de Engenharia Elétrica e Informática
Programa de Pós-Graduação em Engenharia Elétrica

Mapas de Shannon-Kotel'nikov na Distribuição Quântica de Chaves com Variáveis Contínuas

Edmar José do Nascimento

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 grau de Doutor em Ciências no Domínio da Engenharia Elétrica.

Área de Concentração: Processamento da Informação.

Francisco Marcos de Assis
Orientador

Campina Grande – PB, Paraíba, Brasil

©Edmar José do Nascimento

FICHA CATALOGRÁFICA ELABORADA PELA BIBLIOTECA CENTRAL DA UFCG

N244m Nascimento, Edmar José do.
Mapas de Shannon-Kotel'nikov na distribuição quântica de Chaves com Variáveis Contínuas / Edmar José do Nascimento. – Campina Grande, 2017.
101 f. : il.

Tese (Doutorado em Engenharia Elétrica) – Universidade Federal de Campina Grande, Centro de Engenharia Elétrica e Informática, 2017.
"Orientação: Prof. Dr. Francisco Marcos de Assis".
Referências.

1. Distribuição Quântica de Chaves com Variáveis Contínuas. 2. Criptografia Quântica. 3. Mapas de Shannon-Kitel'nikov. 4. Modulação não Linear. I. Assis, Francisco Marcos de. II. Título.

CDU 621.3(043)

**"MAPAS DE SHANNON - KOTEL'NIKOV NA DISTRIBUIÇÃO QUÂNTICA DE CHAVES
COM VARIÁVEIS CONTÍNUAS"**


EDMAR JOSÉ DO NASCIMENTO

TESE APROVADA EM 18/04/2017


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


BENEMAR ALENCAR DE SOUZA, D.Sc., UFCG
Examinador(a)


DANIEL FELINTO PIRES BARBOSA, Dr., UFPE
Examinador(a)


DANIEVERTON MORETTI, Dr., UFCG
Examinador(a)


RENATO PORTUGAL, Dr., LNCC
Examinador(a)

CAMPINA GRANDE - PB

Agradecimentos

Agradecer pela realização de um trabalho como uma tese de doutorado é algo difícil, já que ele é o resultado de toda uma formação obtida ao longo da vida, em que as fraquezas e virtudes se tornam evidentes. Além disso, é um trabalho de grande custo físico e emocional para o indivíduo.

Dessa forma, agradeço primeiramente a minha mãe, Maria do Socorro, pelo incentivo dado a minha educação desde que comecei a escrever as primeiras letras. Também agradeço a minha esposa Christiane por estar sempre ao meu lado nos momentos bons e ruins, compartilhando alegrias e tristezas. Não poderia também faltar o agradecimento para os demais familiares: irmãos, irmãs, pai, cunhadas, sogra, entre outros.

Agradeço ao Prof. Francisco Marcos de Assis por me orientar mais uma vez em mais um trabalho, sempre dando a liberdade de escolha temática, o que me permitiu enveredar por domínios desconhecidos, complexos e desafiadores. Na linha acadêmica, ressalto também a importância das contribuições diversas obtidas durante o meu exame de qualificação, que enriqueceram enormemente o trabalho final.

Agradeço também aos colegas professores do CENEL/UNIVASF por permitirem o afastamento de minhas atividades docentes durante o meu doutorado, algo essencial para o sucesso do trabalho.

Por fim, gostaria de agradecer aos coordenadores e a todo o pessoal administrativo da COPELE, pela eficiência ao lidarem com as questões burocráticas.

“A persistência é o menor caminho do êxito.”

—CHARLES CHAPLIN

Resumo

Protocolos para a distribuição quântica de chaves (DQC) permitem que duas partes (Alice e Bob) compartilhem uma chave secreta que pode ser usada para fins criptográficos. A segurança do protocolo é baseada em propriedades da mecânica quântica, ao invés de hipóteses computacionais. Na distribuição quântica de chaves com variáveis contínuas (DQCVC), a informação é codificada nas amplitudes de quadratura do campo eletromagnético quantizado. Quando implementado com variáveis contínuas, o aparato usado na DQC é consideravelmente mais simples que nas implementações convencionais com variáveis discretas, já que se pode utilizar a medição do tipo homódina, ao invés da detecção de fótons. Uma vez realizada a medida, ainda se faz necessária uma etapa de processamento clássico, denominada de reconciliação da informação, a fim de que Alice e Bob possam compartilhar uma cadeia comum de bits. Para que a DQCVC possa ser realizada em distâncias razoáveis (superiores a 30 km), o processo de reconciliação precisa ser feito com eficiências elevadas (superiores a 90%). Entretanto, eficiências dessa ordem para baixas SNRs (*signal-to-noise ratio* - razão sinal ruído) requerem o uso de códigos clássicos de comprimento bastante elevado e, assim, são difíceis de serem alcançadas. Nesta tese, se propõe o uso dos mapas de Shannon-Kotel'nikov na preparação dos estados quânticos que são usados na DQCVC. Com a utilização desses mapas, é possível aumentar a SNR entre Alice e Bob sem aumentar a variância da modulação de Alice. Dessa forma, o processo de reconciliação se torna mais simples, pois eficiências de reconciliação mais altas são mais facilmente alcançadas em SNRs maiores. Como contribuições desta tese têm-se: a proposição de um protocolo; a definição de um cenário de simulação e a análise do protocolo para dois tipos de mapas (a espiral uniforme de Arquimedes e as curvas geodésicas em um toro planar).

Palavras-chave: Distribuição Quântica de Chaves com Variáveis Contínuas, Criptografia Quântica, Mapas de Shannon-Kotel'nikov, Modulação não Linear.

Abstract

Quantum key distribution (QKD) protocols allow two parties, Alice and Bob, to share a secret key that may be used for cryptographic purposes. The security of QKD is based on quantum mechanics properties instead of computational assumptions. In continuous-variable quantum key distribution (CVQKD), the information is encoded in the quadrature amplitudes of the quantized electromagnetic field. When QKD is implemented with continuous variables, hardware components are much simpler than their discrete variables equivalents. This is mainly due to homodyne detection instead of photon detection. After measuring the transmitted states, it is still necessary to carry out a classical processing stage known as information reconciliation. This stage allows Alice and Bob to share a common sequence of bits. In order to deploy CVQKD over reasonable distances (over 30 km), reconciliation must be done at high efficiencies (over 90%). However, such high efficiencies for low SNRs (*signal-to-noise ratio*) require long length classical codes and are difficult to be reached. In this thesis, we propose to use Shannon-Kotel'nikov maps for preparing quantum states in CVQKD. By using these maps, it is possible to increase the SNR between Alice and Bob, without increasing Alice's variance. Thus, reconciliation becomes easier because higher reconciliation efficiencies are more easily reached for higher SNRs. The contributions of this theses are: the proposal of a CVQKD protocol; the statement of a simulation scenario; the analysis of the proposed protocol for two kinds of maps (uniform Archimedes' spiral and geodesic curves on a flat torus).

Keywords: Continuous Variable Quantum Key Distribution, Quantum Cryptography, Shannon-Kotel'nikov Maps, Non-linear Modulation.

Sumário

1	Introdução	1
1.1	Contribuições	4
1.2	Organização da Tese	5
2	Fundamentação Teórica	6
2.1	Axiomas, Postulados e Definições	6
2.2	Quantização do Campo Eletromagnético	9
2.2.1	Expansão em Modos Normais	11
2.2.2	Modos Monocromáticos	12
2.2.3	Operadores do Campo	13
2.3	Estados do Campo Eletromagnético	14
2.3.1	Estados de Quadratura	14
2.3.2	Estados de Fock	15
2.3.3	Estados Coerentes	18
2.3.4	Estados Comprimidos	19
2.4	Representações no Espaço de Fase	21
2.4.1	Função de Wigner	22
2.4.2	Operações Gaussianas	24
2.4.3	Decomposição de Estados Gaussianos	26
2.5	Medições Ópticas	27
2.5.1	Medições Homódinas	28
2.6	Tópicos de Teoria da Informação	30
2.6.1	Entropias e Informação Mútua	30
2.6.2	Capacidade de Canal	31
3	Protocolos para DQCVC	33
3.1	Visão Geral da DQC	33
3.2	Protocolos para DQCVC	35
3.2.1	Protocolo com Estados Comprimidos	35
3.2.2	Protocolo com Estados Coerentes	38

3.2.3	Protocolo com Medições Heteródinas	44
3.2.4	Protocolos com Modulação Discreta	46
3.2.5	Outros Protocolos	48
3.3	Reconciliação da Informação	49
3.3.1	Protocolo SEC	51
3.3.2	Reconciliação Binária	55
3.3.3	Modulação Codificada	56
3.3.4	Reconciliação para Modulações Discretas	59
3.4	Amplificação de Privacidade	59
4	Mapas de Shannon-Kotel'nikov	61
4.1	Interpretação Geométrica	61
4.1.1	Medidas de Desempenho	62
4.1.2	Aproximação de Baixo Ruído	63
4.2	Espiral Uniforme de Arquimedes	65
4.3	Geodésicas em Toros Planares	67
5	Mapas de Shannon-Kotel'nikov na DQCVC	69
5.1	O Protocolo	69
5.2	Modelo de Simulação	71
5.2.1	Canal	71
5.2.2	Receptor ML	74
5.2.3	Segurança e Estimação da Informação Mútua	74
5.2.4	Dimensionamento das Curvas	75
5.3	Simulações e Resultados	76
5.3.1	Simulações	76
5.3.2	Resultados	76
6	Conclusões e Perspectivas	83
	Referências Bibliográficas	84
A	Lista de Artigos Produzidos	91
B	Código Fonte das Simulações	92
B.1	Espiral Uniforme de Arquimedes	92
B.2	Geodésicas no Toro Planar $N = 4$	95
B.3	Estimador de Kraskov	99

Lista de Figuras

2.1	Medida da quadratura \hat{x} usando detecção homódina ao longo da escala de tempo. O histograma dos dados é mostrado do lado direito (Figura obtida de [36]).	17
2.2	Representação das quadraturas do vácuo. O círculo indica que as flutuações de \hat{x} e \hat{p} são idênticas.	17
2.3	Representação das quadraturas de um estado coerente $ \alpha\rangle$. Um estado coerente pode ser interpretado como o vácuo deslocado.	19
2.4	Representação das quadraturas do vácuo comprimido. Nesse caso, a quadratura x é comprimida enquanto que a quadratura p é expandida.	20
2.5	Função de Wigner para o vácuo. Nota-se que ela corresponde a uma gaussiana bidimensional.	25
2.6	Representação de um divisor de feixe (BS) de transmissividade τ . Os modos de entrada \hat{a}_1 e \hat{a}_2 são combinados no BS resultando nos modos de saída \hat{a}'_1 (transmitido) e \hat{a}'_2 (refletido).	26
2.7	Representação da medição simultânea de ambas as quadraturas de um mesmo modo eletromagnético. O sinal é dividido em um BS balanceado. Nos modos de saída são medidas as quadraturas \hat{x} e \hat{p}	28
2.8	Esquema geral de um detector homódino. O sinal a ser medido e o oscilador local são combinados em um divisor de feixe. Os feixes de saída passam por um fotodetector gerando uma corrente elétrica. A quadratura a ser medida é proporcional à diferença das correntes.	29
3.1	A quadratura \hat{x} do vácuo comprimido é deslocada de um valor x_0 escolhido de acordo com uma distribuição gaussiana de média nula e variância Σ_1^2	36
3.2	Taxa de geração de chave ΔI em função de V_A unidades de N_0 para $\chi = 1/2$ ($T = 2/3$).	40
3.3	Gráfico de ΔI_{RR} versus $1 - T$ para diferentes valores do excesso de ruído e $V_A = 20$ ($V = 21$). Nota-se que com o aumento de ϵ , ΔI_{RR} diminui, mas permanece positiva, desde que $\epsilon < 1/2$	43

3.4	Versão EB da DQCVC. Alice prepara um estado emaranhado (EPR), envia uma metade a Bob e realiza uma medição na sua parte. Dependendo do parâmetros usados por Alice, o protocolo pode ser equivalente ao de estados comprimidos ou ao de estados coerentes. Figura obtida de [21].	43
3.5	Protocolo NS. Bob mede as quadraturas do modo B' . Uma estratégia de espionagem genérica consiste em uma transformação S no modo de Alice e em dois modos auxiliares do vácuo. Figura obtida de [69].	46
3.6	Esquema de codificação usado para o protocolo de dois (esquerda) e de quatro estados (direita). Figura obtida de [74].	47
3.7	Efeito da eficiência de reconciliação nas taxas de geração de chave ΔI em função da distância para o protocolo GG02 sob ataques coletivos. Nesses gráficos, considera-se que a atenuação do canal vale $0,2 \text{ dB/km}$ ($T = 10^{(-0,02d)}$, d em km) e $\epsilon = 0,02$. Na esquerda, $V_A = 10$. Na direita, $V_A = 20$	49
3.8	Ilustração das etapas do protocolo SEC. A cada etapa um BCP é utilizado de modo a reconciliar as sequências binárias geradas por Alice e Bob.	51
3.9	Distribuições $\Pr[S_1(X) = 0 Y = y]$ à esquerda e $\Pr[S_1(X) = 1 Y = y]$	55
3.10	Reconciliação como um problema de codificação de canal.	57
3.11	Reconciliação com BICM. Os dados de Alice são quantizados (Q), mapeados em bits (L) e entrelaçados (Π). O codificador calcula a síndrome da sequência de símbolos, que é enviada a Bob. Bob decodifica seus dados iterativamente usando a síndrome recebida e uma função dos seus dados (Λ).	57
3.12	Reconciliação com MLC/MSD. Figura adaptada de [22].	58
4.1	Símbolos da fonte m são mapeados pelo transmissor em formas de onda $s_m(t)$. O receptor produz uma estimativa \hat{m} dos símbolos transmitidos com base no sinal ruidoso recebido $r(t)$	62
4.2	Representação genérica de um mapeamento 1:2. Os símbolos da fonte $m \in [-1, 1]$ são mapeados em formas de onda do canal. A ponta do vetor $s(m)$ percorre o <i>locus</i> do sinal. O círculo tracejado indica a restrição de potência do canal.	63
4.3	Limitante OPTA em função da razão N/M	64
4.4	Gráfico de uma espiral uniforme de Aquimedes. As linhas tracejadas correspondem ao mapeamento de valores negativos, enquanto as linhas sólidas correspondem ao mapeamento de valores positivos.	66
5.1	Diagrama de blocos do protocolo proposto. Pontos de uma curva são usados para a preparação dos estados coerentes enviados por Alice. Bob e Eva obtém cada um a sua estimativa do parâmetro escolhido por Alice a partir de seus receptores ML.	70

-
- 5.2 Diagrama de blocos para as variáveis de quadratura. As quadraturas de Alice e Bob são denotadas por (x_A, p_A) e (x_B, p_B) , respectivamente. (x_{in}, p_{in}) e (x_{out}, p_{out}) denotam as quadraturas na entrada e na saída do canal, respectivamente. 71
- 5.3 Ataque do tipo feedforward. Eva captura uma fração $1 - T_E$ do sinal de entrada. Ela então mede ambas as quadraturas desta fração. Os resultados de sua medida são usados para transladar a fração transmitida T_E do sinal de entrada. 73
- 5.4 Valores simulados para a $SDR_{AB} = \sigma_m^2/D$ comparados com a $CSNR_{AB}$ para o protocolo NS. Observa-se que a diferença entre SDR_{AB} e $CSNR_{AB}$ aumenta para CSNRs mais elevadas (valores maiores de T). 77
- 5.5 No gráfico superior, as informações mútuas I_{AB}^{SK} e I_{AE}^{SK} são comparadas. Pode-se notar que $I_{AB}^{SK} > I_{AE}^{SK}$ para $T > 0,57$. No gráfico inferior, as informações mútuas I_{AB}^{SK} e I_{BE}^{SK} são comparadas. Nota-se que $I_{AB}^{SK} > I_{BE}^{SK}$ para os valores simulados. 78
- 5.6 Valores simulados para a SDR são comparados a CSNR. O subscrito *sp* se refere à espiral enquanto que $4D$ e $6D$ se referem à dimensão da curva no toro. É possível notar a tendência de ganhos mais elevados para mapas em dimensões maiores. 79
- 5.7 Valores simulados para as informações mútuas para o protocolo proposto. No lado esquerdo, é mostrado o caso da reconciliação direta. No lado direito, é mostrado o caso da reconciliação reversa. (a) e (b) foram obtidos para a espiral de Arquimedes. (c),(d) e (e),(f) foram obtidos para as geodésicas no toro planar para $N = 4$ e $N = 6$, respectivamente. 80
- 5.8 Eficiências mínimas de reconciliação são mostradas para a reconciliação direta (a) e reversa (b). Os valores simulados são comparados com o protocolo NS (linhas sólidas vermelhas). É possível notar que o protocolo proposto requer protocolos de reconciliação mais eficientes para um dado T . Esse efeito se torna mais evidente para SNRs mais elevadas. 81

Lista de Tabelas

2.1	Diferentes representações para os operadores de quadratura do campo.	15
-----	------------------------------------------------------------------------------	----

Lista de Siglas

AWGN - Ruído Aditivo Gaussiano Branco (*Additive White Gaussian Noise*)

BCP - Protocolo de Correção Binária (*Binary Correction Protocol*)

BICM - Modulação Codificada com Bits Entrelaçados (*Bit Interleaved Coded Modulation*)

BS - Divisor de Feixe (*Beam Splitter*)

CVQKD - *Continuous-Variable Quantum Key Distribution*

CSNR - Razão Sinal-Ruído do Canal (*Channel Signal-to-Noise Ratio*)

DQC - Distribuição Quântica de Chaves

DQCVK - Distribuição Quântica de Chaves com Variáveis Contínuas

EB - Baseada em Emaranhamento (*Entanglement-Based*)

FM - Modulação em Frequência (*Frequency Modulation*)

GG02 - Grosshans e Grangier 2002

LDPC - Códigos de Checagem de Paridade com Baixa Densidade (*Low-Density Parity Check Codes*)

ML - Máxima Verossimilhança (*Maximum Likelihood*)

MLC/MSD - Codificação Multinível/Decodificação Multiestágio (*MultiLevel Coding/Multi-Stage Decoding*)

MSE - Erro Quadrático Médio (*Mean Squared Error*)

NLA - Amplificador Linear sem Ruído (*Noiseless Linear Amplifier*)

NS - Sem Comutação (*No-Switching*)

OPTA - Desempenho Ótimo Teoricamente Alcançável (*Optimal Performance Theoretically Attainable*)

POVM - Medida com Operadores Positivos (*Positive Operator-Valued Measure*)

QKD - *Quantum Key Distribution*

RD - Reconciliação Direta

RR - Reconciliação Reversa

SDR - Razão Fonte-Distorção (*Source-to-Distortion Ratio*)

SEC - Correção de Erros Fatiada (*Sliced Error Correction*)

SK - Shannon-Kotel'nikov

SNR - Razão Sinal-Ruído (*Signal-to-Noise Ratio*)

CAPÍTULO 1

Introdução

Um dos objetivos da criptografia é permitir que duas partes legítimas (Alice e Bob) possam se comunicar sob sigilo, mesmo quando as mensagens trocadas estão sujeitas à interceptação por uma terceira parte não autorizada (Eva). Para isso, Alice e Bob fazem uso de um algoritmo para cifrar e decifrar as suas mensagens e de uma chave secreta¹. Supõe-se que o algoritmo seja de conhecimento público, sendo o sigilo provido apenas pelo desconhecimento de Eva acerca da chave secreta utilizada no processo de cifragem.

A segurança do sistema criptográfico depende da definição de segurança adotada e das hipóteses de utilização do sistema que são admitidas. Um dos critérios de segurança que pode ser utilizado é o de sigilo perfeito (*perfect secrecy*) introduzido por Shannon em [1]. De acordo com esse critério, o texto cifrado não deve revelar nenhuma informação acerca do texto original. Como consequência dessa hipótese, a chave utilizada deve ser aleatória, de tamanho maior ou igual ao texto a ser cifrado e deve ser usada apenas uma única vez [2]. Critérios de segurança mais fracos, baseados em complexidade computacional, permitem que a chave seja reutilizada certo número de vezes e que o tamanho dessa chave seja inferior ao do texto a ser cifrado.

Independentemente do critério de segurança adotado, resta ainda o problema de distribuição das chaves, ou seja, como Alice e Bob podem compartilhar uma chave secreta, mesmo estando o canal de comunicação usado por eles sujeito à interceptação. Na maioria das transações eletrônicas realizadas atualmente através da Internet, a chave é distribuída através de um sistema de criptografia assimétrica como o RSA (Rivest, Shamir e Adleman). No RSA, utiliza-se um par de chaves distintas, de modo que uma mensagem cifrada com uma delas só pode ser decifrada com a outra. Assim, para finalidades de criptografia, uma dessas chaves é disponibilizada publicamente, enquanto a outra é mantida privada. Dessa forma, Alice pode gerar uma chave secreta e cifrá-la com a chave pública de Bob usando o RSA. Bob, por sua vez, aplica o seu par privado e assim, a chave secreta gerada por Alice é compartilhada com Bob [3]. Apesar de ser amplamente usado nos dias atuais, o RSA tem a sua segurança baseada em hipóteses

¹A chave secreta corresponde a uma sequência de bits compartilhada entre Alice e Bob e que deve ser mantida em sigilo.

computacionais não provadas. Particularmente, acredita-se que a segurança do sistema resida na dificuldade de se fatorar produtos de números primos em seus fatores. Assim, a descoberta de um algoritmo de fatoração mais eficiente poderia comprometer a sua segurança. Além do RSA, há ainda a possibilidade de se entregar uma cópia da chave fisicamente. Essa solução foi empregada em diversas situações ao longo da história, principalmente na criptografia para fins militares [4].

Dentre os métodos de distribuição de chaves, a distribuição quântica de chaves (DQC) se destaca por ter a sua segurança baseada nas leis da mecânica quântica, ao invés de hipóteses computacionais [5]. Segundo a mecânica quântica, quando se tenta ter acesso à informação representada em um estado quântico genérico, realiza-se uma perturbação nesse estado. Essa propriedade quântica tem como consequências a possibilidade de que tentativas de espionagem sejam detectadas ou ainda que não seja possível a criação de cópias perfeitas de estados não ortogonais [6]. Dessa forma, a DQC permite que Alice e Bob compartilhem uma chave secreta mesmo estando separados fisicamente e ligados através de um canal de comunicação inseguro.

Os primeiros protocolos para DQC foram concebidos para sistemas quânticos de dois níveis (variáveis discretas). Nesses protocolos, a informação é codificada na polarização de fótons² (polarização horizontal-vertical ou em uma base conjugada) e APDs (*Avalanche Photodiodes*) são usados para detectar a presença ou a ausência de fótons na base medida. Exemplos de tais protocolos são os tradicionais BB84 [7], o B92 [8] e o EPR (Einstein-Podolsky-Rosen) [9]. Se não forem levadas em conta as imperfeições de uma implementação física, o BB84 é provado seguro incondicionalmente [10].

Do ponto de vista experimental, a implementação de protocolos como o BB84 requer uma aparelhagem óptica especializada: geradores de fótons únicos e APDs de grande eficiência³. Uma das grandes limitações na velocidade de geração de bits da chave está na eficiência dos APDs. No comprimento de onda de 1550 nm usado nas comunicações ópticas clássicas, a eficiência dos APDs ainda é muito baixa. Além disso, as implementações práticas são realizadas com pulsos fortemente atenuados, o que deixa o protocolo vulnerável a ataques quando mais de um fóton é emitido [11]. Felizmente, esse tipo de vulnerabilidade pode ser corrigida com o uso dos estados isca (*decoy states*) propostos em [12]. A grande vantagem dessa abordagem é que as condições de segurança podem ser satisfeitas mesmo em regime de perdas elevadas [13]. Em relação à eficiência dos APDs, algumas tecnologias têm se mostrado promissoras: SD (*self-differential*), SG (*sinusoidal gating*) e SSPD (*superconductive single photon detectors*). Com esses avanços, a DQC com variáveis discretas permite gerar chaves a distâncias de até 250 km, apesar de as taxas de geração serem baixas nesses casos e, muitas vezes, requererem um ambiente controlado [14].

²Em implementações práticas usando fibras ópticas, a informação geralmente é codificada na fase, pois a polarização pode ser perdida facilmente com a propagação ao longo da fibra, caso esta não tenha propriedades de manutenção da polarização.

³A eficiência de APDs na detecção de fótons se refere à probabilidade (em percentagem) de que um fóton incidente gere um pulso elétrico na saída do detector.

Por volta do ano 2000 surgiu uma nova abordagem para DQC, que faz uso de variáveis contínuas para representar a informação codificada nos estados quânticos [15, 16]. Na distribuição quântica de chaves com variáveis contínuas (DQCVC), a informação é transportada nas amplitudes de quadratura do campo eletromagnético quantizado. Dessa forma, a DQC pode ser realizada usando estados ópticos coerentes juntamente com medições homódinas das amplitudes de quadratura. Esse aspecto da medição foi o principal apelo dessa técnica, pois ela é realizada com fotodetectores do tipo PIN, que são usados largamente nas comunicações ópticas clássicas, possuindo ainda eficiência elevada e operando na faixa dos giga-hertz [11]. O preço a ser pago na detecção homódina é que a medição das quadraturas é intrinsecamente ruidosa devido ao ruído do vácuo. Nos esquemas discretos baseados em detecção de fótons, há uma espécie de filtragem realizada na medição, já que um sinal fortemente atenuado pelas perdas na linha de transmissão resulta na ausência de cliques nos detectores. Por outro lado, na DQCVC, as perdas na linha juntamente com o ruído do vácuo causam uma diminuição na SNR (*signal-to-noise ratio* - razão sinal-ruído) das quadraturas medidas, tornando a etapa clássica de processamento posterior mais complexa computacionalmente [17].

Em teoria, Alice e Bob podem obter uma chave secreta a partir de dados compartilhados usando DQCVC, desde que a informação mútua de Alice para Bob (I_{AB}) seja maior que a informação mútua de Eva para Alice (I_{AE}) ou para Bob (I_{BE}) [2]. Entretanto, para que essa informação compartilhada entre Alice e Bob resulte em bits de chave, é necessário primeiramente aplicar um protocolo de reconciliação nessas sequências de dados. Se o protocolo de reconciliação for bem sucedido, Alice e Bob devem, ao final dele, compartilhar uma sequência binária de dados comum. Um protocolo de reconciliação para variáveis contínuas deve possuir algum esquema de quantização para os dados, seguido da utilização de códigos corretores de erros [18]. Para que esses códigos possam ser utilizados, é necessário o envio de informação adicional de uma parte para a outra através de um canal público autenticado. Devido ao custo do processo de reconciliação (quantização e informação adicional trocada), a informação mútua presente na sequência binária comum é inferior à informação mútua original I_{AB} . Essa diminuição é traduzida pela eficiência de reconciliação β ($0 < \beta < 1$), de modo que apenas βI_{AB} bits de informação por uso do canal contribuem para a geração da chave.

À medida que a distância entre Alice e Bob aumenta, faz-se necessário uma eficiência de reconciliação cada vez maior para que uma chave secreta possa ser obtida a partir dos dados compartilhados [19]. Além disso, essa eficiência elevada tem que ser obtida em SNRs baixas, já que aumentar a potência do sinal de Alice potencializaria o ganho de informação de Eva, elevando assim ainda mais os requisitos de eficiência de reconciliação [20]. Em [21], a DQCVC foi implementada em um enlace de 25 km de fibra óptica. Nesse caso, a reconciliação foi realizada usando-se a técnica MLC/MSD (*multilevel coding and multistage decoding*) [22] junto com códigos LDPC (*low-density parity check codes*) para blocos de 200.000 bits. Com isso, foi alcançada uma eficiência de reconciliação $\beta = 0,898$ para uma SNR de 3,38 (5,3 dB), resultando em uma taxa final de geração de chave de 2 kb/s. Essa taxa poderia ser pelo menos

seis vezes maior se o processamento dos códigos LDPC não limitasse a taxa final do protocolo [17]. Em trabalhos posteriores, melhorias na eficiência de reconciliação foram alcançadas explorando-se novas técnicas de construção de códigos LDPC. Em [23], alcançou-se $\beta = 0,937$ para uma SNR de 3 (4,77 dB), mantendo-se o mesmo comprimento dos blocos. A extensão de eficiências elevadas para SNRs ainda mais baixas pode ser alcançada usando-se códigos específicos para cada nível do MLC/MSD combinado com o uso de blocos maiores para os códigos LDPC (mais de um milhão de bits). Seguindo essa linha, em [20], alcançou-se $\beta = 0,934$ para uma SNR de 0,55 (-2,6 dB). Além do MLC/MSD, para SNRs baixas, é possível utilizar o método denominado de reconciliação multidimensional, que permite converter o canal usual com entradas gaussianas em um canal com entradas binárias [24,25]. Com isso, códigos LDPC otimizados para esse tipo de canal permitem que se alcancem eficiências de reconciliação elevadas em regiões de baixa SNR. Com o uso da reconciliação multidimensional, foi possível implementar a DQCVC em um enlace de fibra óptica de 80 km [26].

As eficiências máximas de reconciliação alcançáveis aumentam de acordo com a SNR, assim como indicado em uma fórmula empírica apresentada em [27]. Dessa forma, outra maneira de melhorar o desempenho da DQCVC seria através do aumento da SNR no aparato de Bob sem que houvesse aumento da potência do sinal de Alice. Essa abordagem tornou-se teoricamente possível com o conceito de NLA⁴ (*noiseless linear amplifier* - amplificador linear sem ruído) proposto em [28]. Com o NLA, seria possível amplificar o sinal recebido por Bob sem a introdução de ruído no processo. No contexto da DQCVC, para o protocolo GG02 [19], mostra-se que um NLA ideal de ganho g permitiria perdas adicionais na linha de $20 \log_{10} g^2$ dB antes que a taxa de geração de chave caísse para zero [29]. Quando imperfeições são consideradas no modelo do NLA, simulações realizadas para o protocolo NS (*no-switching*) [30] mostram que um NLA ainda proporcionaria ganhos em distância e excesso de ruído tolerado [31].

1.1 Contribuições

As contribuições propostas nesta tese de doutorado têm como objetivo melhorar o desempenho da DQCVC utilizando esquemas de modulação não lineares na preparação de estados coerentes. Na escolha e caracterização desses esquemas de modulação, faz-se uso de uma interpretação geométrica descrita em [32,33]. Assim, a preparação de estados coerentes pode ser interpretada com um mapeamento de um determinado parâmetro em um ponto pertencente a uma curva em um espaço N -dimensional. As quadraturas medidas por Bob são interpretadas com um ponto ruidoso que deve ser projetado na curva a fim de que uma estimativa do parâmetro transmitido seja obtida. Com a escolha de um mapeamento apropriado, podem-se

⁴O NLA é um amplificador probabilístico em que o evento amplificação ocorre com determinada probabilidade, sendo que essa probabilidade é menor para ganhos maiores. No NLA, os eventos de sucesso ou fracasso são sinalizados pela medição de estados auxiliares.

mitigar os efeitos do ruído, aumentando-se a fidelidade entre o parâmetro e a sua estimativa e, consequentemente, elevando-se a SNR entre as variáveis de Alice e Bob⁵.

A utilização de mapeamentos não lineares na DQCVC foi proposta inicialmente em [34]. Nesse artigo, a espiral uniforme de Arquimedes foi utilizada como mapeamento, tendo como objetivo explorar o efeito de limiar na detecção de ações de espionagem. Posteriormente, em [35], um protocolo foi formalmente descrito e a sua segurança foi avaliada para um ataque de alimentação direta (*feedforward*). Simulações realizadas com a espiral uniforme de Arquimedes como mapeamento mostraram que é possível usar essa construção na DQCVC e que ela proporciona ganhos na SNR calculada por Bob. Ainda nesta tese, são reportados resultados obtidos com o protocolo proposto usando curvas em um toro planar. Essas curvas estão inseridas em espaços de dimensões maiores ($N = 2k$, $k = 2, 3, \dots$) que a espiral de Arquimedes ($N = 2$), o que permite explorar SNRs menores (distâncias maiores).

1.2 Organização da Tese

O restante desta tese está organizado da seguinte forma:

- No capítulo 2, a terminologia e a fundamentação teórica relacionadas aos protocolos de distribuição quântica de chaves são introduzidas. São discutidos tópicos como a quantização do campo eletromagnético, as ferramentas de análise no espaço de fase, a caracterização das medidas, além de tópicos ligados à teoria da informação.
- No capítulo 3, é apresentada uma revisão acerca dos principais protocolos usados na DQCVC.
- No capítulo 4, descreve-se a interpretação geométrica das modulações não lineares. Além disso, são analisados os mapeamentos usados no protocolo proposto nesta tese.
- No capítulo 5, as contribuições propostas nesta tese são detalhadas.
- No capítulo 6, são apresentadas algumas conclusões sobre os trabalhos realizados, bem como possibilidades para trabalhos futuros.
- No apêndice A, enumera-se a produção bibliográfica realizada ao longo deste trabalho de tese.
- No apêndice B, tem-se a transcrição de parte do código fonte usado nas simulações realizadas para esta tese.

⁵As variáveis de Alice e Bob correspondem ao parâmetro e a sua estimativa, respectivamente. Nos protocolos convencionais, as variáveis correspondem aos valores das quadraturas.

CAPÍTULO 2

Fundamentação Teórica

Neste capítulo, são introduzidas as ferramentas necessárias ao entendimento dos protocolos usados na DQCVC. Inicialmente, são apresentados os axiomas da mecânica quântica juntamente com algumas notações e terminologias necessárias. Em seguida, realiza-se a quantização do campo eletromagnético, introduzindo-se assim os operadores de campo, além da representação no espaço de fase. São apresentados também alguns modelos de componentes ópticos básicos e esquemas de medição que são normalmente utilizados. Por fim, são relacionados alguns tópicos da teoria da informação clássica e quântica, que são usados no contexto da DQCVC. A descrição aqui representada é baseada em textos tradicionais de óptica quântica tais como [36–41], além dos artigos de revisão [15, 16] e teses de doutorado [42–44].

2.1 Axiomas, Postulados e Definições

A óptica quântica tem como teoria subjacente a mecânica quântica. Esta, por sua vez, tem como base um conjunto de axiomas ou postulados que proveem uma estrutura matemática para descrever os sistemas físicos. A formulação em quatro postulados descrita nesta seção foi proposta em [45], sendo bastante similar à apresentada em [36]. Essa formulação não é única. Em [37], por exemplo, a mecânica quântica é descrita por cinco axiomas. Além dos postulados, são introduzidas algumas notações e definições que são usadas ao longo do texto.

Postulado 2.1. *A qualquer sistema físico isolado existe associado um espaço vetorial complexo com produto interno (ou seja, um espaço de Hilbert), conhecido como espaço de estados do sistema. O sistema é completamente descrito pelo seu vetor de estado, um vetor unitário no espaço de estados.*

Na notação de Dirac, o estado de um objeto quântico perfeitamente preparado (um estado puro) é denotado por $|\psi\rangle$. Superposições do tipo $c_1|\psi_1\rangle + c_2|\psi_2\rangle$, em que $|\psi_1\rangle$ e $|\psi_2\rangle$ são estados ortonormais e c_1 e c_2 são números complexos ($|c_1|^2 + |c_2|^2 = 1$), também são estados possíveis. Ainda segundo a notação de Dirac, $\langle\psi|$ representa o vetor dual (conjugado trans-

posto) de $|\psi\rangle$. Dessa forma, o produto escalar entre os vetores $|\varphi\rangle$ e $|\psi\rangle$ é convenientemente representado por $\langle\varphi|\psi\rangle$.

A descrição de sistemas quânticos por um vetor de estados $|\psi\rangle$ é conveniente para a representação de estados puros. No caso mais geral, quando o estado do sistema quântico não é completamente conhecido, descreve-se o estado do sistema através de um operador densidade denotado por $\hat{\rho}$. Esse desconhecimento sobre o estado se deve principalmente às incertezas na sua preparação. Para um sistema quântico que pode estar em um dentre muitos estados $|\psi_i\rangle$ (uma mistura de estados) com probabilidade p_i , o operador densidade é definido por:

$$\hat{\rho} \equiv \sum_i p_i |\psi_i\rangle \langle\psi_i|, \text{ com } \sum_i p_i = 1. \quad (2.1)$$

No caso específico de um estado puro $|\psi\rangle$, o operador densidade é dado simplesmente por $\hat{\rho} = |\psi\rangle \langle\psi|$.

Postulado 2.2. *As medidas quânticas são descritas por determinados operadores de medida $\{\hat{M}_m\}$. Esses operadores atuam sobre o espaço de estados do sistema. O índice m se refere aos possíveis resultados da medida. Se o estado de um sistema quântico for dado por $|\psi\rangle$ imediatamente antes da medida, a probabilidade de um resultado m ocorrer é dada por:*

$$p(m) = \|\hat{M}_m |\psi\rangle\|^2, \quad (2.2)$$

e o estado do sistema após a medida será:

$$|\psi'\rangle = \frac{\hat{M}_m |\psi\rangle}{\sqrt{p(m)}}. \quad (2.3)$$

Os operadores de medida satisfazem a relação de completitude:

$$\sum_m \hat{M}_m^\dagger \hat{M}_m = \hat{I}. \quad (2.4)$$

Neste postulado, \hat{M}_m^\dagger denota o operador adjunto (conjugado hermitiano) de \hat{M}_m e \hat{I} o operador identidade. A equação (2.4) garante que a soma das probabilidades dos resultados da medida seja um. Relacionado ao postulado 2.2 está o conceito de observável. Um observável é definido como uma propriedade de um sistema físico que, em princípio, pode ser medida, tal como a posição ou o momentum de uma partícula. Na mecânica quântica, um observável é representado por um operador autoadjunto (hermitiano), ou seja, um operador \hat{A} tal que $\hat{A} = \hat{A}^\dagger$. Um operador autoadjunto em um espaço de Hilbert \mathcal{H} possui uma representação espectral, ou seja, os seus autoestados formam uma base ortonormal completa em \mathcal{H} , ou seja:

$$\hat{A} = \sum_n \lambda_n \hat{P}_n = \sum_n \lambda_n |n\rangle \langle n|. \quad (2.5)$$

Em que λ_n é um autovalor de \hat{A} e $\hat{P}_n = |n\rangle\langle n|$ é a projeção ortogonal correspondente no espaço dos autovetores com autovalor λ_n . O conjunto de todos os autovalores de um dado operador é denominado de espectro, que pode ser contínuo ou discreto. As medidas quânticas obtidas através de projetores \hat{P}_n são conhecidas como medidas projetivas, ortogonais ou de Von Neumann. Ao medir um sistema quântico descrito por $|\psi\rangle$, a saída numérica do processo de medição de um observável \hat{A} é um de seus autovalores λ_n , o que ocorre com probabilidade $p(\lambda_n) = \|\hat{P}_n|\psi\rangle\|^2$. Nesse caso, o estado pósmedição passa a ser um dos autoestados $|n\rangle$ do operador \hat{A} .

Como o resultado da medição de um sistema quântico é inerentemente probabilística, é de interesse na análise desses sistemas o cálculo de momentos estatísticos tais como a média e a variância. A interpretação de uma média estatística nesse caso pressupõe a medição de um observável para um conjunto de estados preparados de modo idêntico. Para um estado puro $|\psi\rangle$, a média e a variância de um observável \hat{A} são denotadas, respectivamente, por:

$$\langle \hat{A} \rangle_\psi = \langle \psi | \hat{A} | \psi \rangle, \quad (2.6)$$

$$(\Delta \hat{A})_\psi^2 = \langle \hat{A}^2 \rangle_\psi - (\langle \hat{A} \rangle_\psi)^2 = \langle \psi | \hat{A}^2 | \psi \rangle - \langle \psi | \hat{A} | \psi \rangle^2. \quad (2.7)$$

Ainda relacionado ao postulado 2.2 está o conceito de comutação. Dois operadores \hat{A} e \hat{B} comutam se, e somente se, eles compartilham o mesmo conjunto de autoestados, ou seja, se o comutador definido por

$$[\hat{A}, \hat{B}] \equiv \hat{A}\hat{B} - \hat{B}\hat{A} \quad (2.8)$$

é igual a zero. Se os observáveis não comutam ($[\hat{A}, \hat{B}] \neq 0$), então os observáveis são ditos ser incompatíveis. Nesse caso, eles causam incerteza estatística mútua nos resultados de suas medições. Essa incerteza é quantificada através do princípio de incerteza de Heisenberg, que pode ser formulado como:

$$(\Delta \hat{A})_\psi (\Delta \hat{B})_\psi \geq \frac{1}{2} | \langle [\hat{A}, \hat{B}] \rangle_\psi |. \quad (2.9)$$

Postulado 2.3. *O espaço de estados de um sistema físico composto é o produto tensorial dos estados dos sistemas físicos individuais. Se os sistemas forem numerados de 1 até n, e o sistema i for preparado no estado $|\psi_i\rangle$, decorre que o estado do sistema composto será $|\psi_1\rangle \otimes |\psi_2\rangle \otimes \dots \otimes |\psi_n\rangle$.*

A interação de dois ou mais sistemas quânticos pode criar uma correlação não local entre eles. Essa correlação, que não existe nos sistemas clássicos, é chamada de emaranhamento ou entrelaçamento (*entanglement*). Um estado $|\psi\rangle$ definido em um espaço de Hilbert $\mathcal{H}_A \otimes \mathcal{H}_B$ é considerado emaranhado se ele não puder ser escrito como um produto tensorial de estados $|\phi\rangle \in \mathcal{H}_A$ e $|\varphi\rangle \in \mathcal{H}_B$, ou seja, se $|\psi\rangle \neq |\phi\rangle \otimes |\varphi\rangle$.

Postulado 2.4. A evolução de um sistema quântico fechado é descrita por uma transformação unitária. Ou seja, o estado $|\psi\rangle$ de um sistema em um tempo t_1 está relacionado ao estado $|\psi'\rangle$ do sistema em t_2 por um operador unitário \hat{U} que depende somente de t_1 e t_2 :

$$|\psi'\rangle = \hat{U} |\psi\rangle \quad (2.10)$$

A operação unitária \hat{U} indicada em (2.10) depende do operador de energia do sistema \hat{H} , denominado de Hamiltoniano. Para um Hamiltoniano que independe do tempo, a transformação unitária \hat{U} é dada por

$$\hat{U}(t) = \exp\left(-\frac{i}{\hbar}\hat{H}t\right), \quad (2.11)$$

sendo $\hbar = h/(2\pi)$, em que h é a constante de Planck.

O postulado 2.4 está de acordo com a representação de Schrödinger, na qual o estado evolui enquanto os observáveis permanecem fixos. Na óptica quântica, é conveniente usar a representação de Heisenberg, na qual os operadores evoluem enquanto o estado permanece fixo. Em ambas as representações, as quantidades que são medidas em sistemas quânticos como a média (2.6) e a variância (2.7) são equivalentes. Na representação de Heisenberg, um operador com representação de Schrödinger \hat{A} é definido como

$$A(t) = \hat{U}^\dagger(t)\hat{A}\hat{U}(t), \quad (2.12)$$

enquanto o estado do sistema é aquele no momento em que $t = 0$. A evolução do operador $A(t)$ é governada pela equação de movimento de Heisenberg que é dada por:

$$\frac{d}{dt}\hat{A}(t) = \frac{i}{\hbar}[\hat{H}, \hat{A}]. \quad (2.13)$$

Essa expressão é válida quando \hat{A} não possui dependência explícita do tempo.

2.2 Quantização do Campo Eletromagnético

A descrição quântica do campo eletromagnético tem como ponto de partida a sua descrição clássica através das equações de Maxwell. A ideia central é que campos clássicos podem ser associados com observáveis quânticos e que, juntamente com as relações de comutação envolvendo esses observáveis, se possa ter uma descrição quântica do campo eletromagnético. O procedimento detalhado a seguir segue a abordagem adotada em [36].

As equações de Maxwell na sua forma macroscópica são dadas por [36]:

$$\nabla \cdot \mathbf{B} = 0, \quad (2.14)$$

$$\nabla \times \mathbf{E} = -\frac{\partial \mathbf{B}}{\partial t}, \quad (2.15)$$

$$\nabla \cdot \mathbf{D} = 0, \quad (2.16)$$

$$\nabla \times \mathbf{H} = \frac{\partial \mathbf{D}}{\partial t}. \quad (2.17)$$

Em que os campos vetoriais indicados em negrito são: \mathbf{B} - indução magnética; \mathbf{H} - campo magnetizante; \mathbf{D} - deslocamento elétrico e \mathbf{E} - campo elétrico. Além dessas quatro equações, é necessário precisar a resposta do meio através das equações constitutivas. Para um meio não absorvente, não dispersivo e isotrópico, as equações constitutivas são dadas por:

$$\mathbf{D} = \varepsilon_0 \varepsilon \mathbf{E}, \quad (2.18)$$

$$\mathbf{B} = \mu_0 \mu \mathbf{H}. \quad (2.19)$$

Sendo ε_0 e μ_0 as permeabilidades elétrica e magnética do vácuo, respectivamente e ε e μ as permeabilidades do meio. Tem-se ainda a relação $c^{-2} = \varepsilon_0 \mu_0$, em que c é a velocidade da luz no vácuo.

Quando se trata de eletromagnetismo quântico, é conveniente a utilização do potencial vetor \mathbf{A} , que é descrito através das equações

$$\mathbf{E} = -\frac{\partial \mathbf{A}}{\partial t}, \quad (2.20)$$

$$\mathbf{B} = \nabla \times \mathbf{A}, \quad (2.21)$$

juntamente com a condição de calibre de Coulomb

$$\nabla \cdot \varepsilon \mathbf{A} = 0. \quad (2.22)$$

Essas três equações satisfazem as equações de Maxwell (2.14-2.16), de forma que a equação (2.17) é a única não trivial. A partir das equações (2.20) e (2.21) e das equações constitutivas, a equação (2.17) resulta na equação de onda dada por:

$$\frac{1}{\mu \varepsilon} \nabla^2 \mathbf{A} - \frac{1}{c^2} \frac{\partial^2 \mathbf{A}}{\partial t^2} = 0. \quad (2.23)$$

O ponto de partida para a quantização do campo consiste em se associar os campos clássicos a médias de operadores quânticos. Assim, por exemplo, o campo elétrico \mathbf{E} pode ser encarado como a média $\langle \psi | \hat{\mathbf{E}} | \psi \rangle$ do operador $\hat{\mathbf{E}}$. Devido a linearidade das equações de Maxwell, verifica-se que se forem feitas as substituições dos campos por operadores ($\hat{\mathbf{E}}$, $\hat{\mathbf{D}}$, $\hat{\mathbf{B}}$,

$\hat{\mathbf{H}}$ e $\hat{\mathbf{A}}$), as médias dos operadores ainda verificam as equações de Maxwell. Assim, o operador potencial $\hat{\mathbf{A}}$ pode ser descrito pelas equações

$$\frac{1}{\mu\varepsilon}\nabla^2\hat{\mathbf{A}} - \frac{1}{c^2}\frac{\partial^2\hat{\mathbf{A}}}{\partial t^2} = 0, \quad (2.24)$$

$$\nabla \cdot \varepsilon\hat{\mathbf{A}} = 0. \quad (2.25)$$

A evolução dos operadores de campo ao longo do tempo também pode ser descrita através das equações de movimento de Heisenberg (2.13). Para isso, é necessário especificar o Hamiltoniano do sistema, bem como as relações de comutação entre os operadores e o Hamiltoniano. Usando a equivalência entre campos e operadores, o Hamiltoniano pode ser escrito como

$$\hat{H} = \frac{1}{2} \int (\hat{\mathbf{E}} \cdot \hat{\mathbf{D}} + \hat{\mathbf{B}} \cdot \hat{\mathbf{H}}) dV = \int \left(\frac{\hat{\mathbf{D}}^2}{2\varepsilon_0\varepsilon} + \frac{\varepsilon_0 c^2}{2\mu} (\nabla \times \hat{\mathbf{A}})^2 \right) dV, \quad (2.26)$$

em que o volume de integração abrange todo o espaço. Usando a equação de movimento de Heisenberg e a relação de comutação entre $\hat{\mathbf{D}}$ e $\hat{\mathbf{A}}$, cujo desenvolvimento não será detalhado neste texto, é possível obter a equação de onda (2.24) para o operador potencial $\hat{\mathbf{A}}$.

2.2.1 Expansão em Modos Normais

No caso clássico, soluções para a equação (2.23) são funções complexas \mathbf{A}_k do espaço e do tempo. Como as equações de Maxwell são reais, as soluções do tipo \mathbf{A}_k^* também fazem parte do conjunto de soluções. De forma análoga, como o operador potencial $\hat{\mathbf{A}}$ é hermitiano, as soluções para a equação (2.24) podem ser expandidas como

$$\hat{\mathbf{A}}(\mathbf{r}, t) = \sum_k \left(\mathbf{A}_k(\mathbf{r}, t) \hat{a}_k + \mathbf{A}_k^*(\mathbf{r}, t) \hat{a}_k^\dagger \right). \quad (2.27)$$

Nessa notação, \mathbf{r} representa a posição no espaço. Os termos \hat{a}_k e \hat{a}_k^\dagger são operadores que carregam as propriedades quânticas do campo, sendo \hat{a}_k^\dagger o conjugado hermitiano de \hat{a}_k . As funções $\mathbf{A}_k(\mathbf{r}, t)$ são denominadas modos, sendo k o índice usado para identificar o modo. Cada modo pode corresponder a determinados números de onda, frequências e polarizações. A expansão dada pela equação (2.27) é denominada de expansão em modos do campo eletromagnético.

Normalmente, são impostas restrições aos modos $\mathbf{A}_k(\mathbf{r}, t)$ a fim de que se tenha relações de comutação mais simples. Uma dessas restrições é que esses modos sejam ortonormais segundo um produto interno definido por

$$(\mathbf{A}_1, \mathbf{A}_2) \equiv \frac{1}{i\hbar} \int (\mathbf{A}_1^* \cdot \mathbf{D}_2 - \mathbf{A}_2 \cdot \mathbf{D}_1^*) dV, \quad \mathbf{D} = -\varepsilon_0\varepsilon \frac{\partial \mathbf{A}}{\partial t}. \quad (2.28)$$

Ou seja, que os modos verifiquem as relações

$$(\mathbf{A}_k, \mathbf{A}_{k'}) = \delta_{kk'}, (\mathbf{A}_k, \mathbf{A}_{k'}^*) = 0, \quad (2.29)$$

em que $\delta_{kk'} = 1$ para $k = k'$ ou $\delta_{kk'} = 0$ para $k \neq k'$. Os modos assim definidos são denominados de modos normais. Para modos normais, os operadores \hat{a}_k e \hat{a}_k^\dagger são calculados como

$$\hat{a}_k = (\mathbf{A}_k, \mathbf{A}), \quad \hat{a}_k^\dagger = -(\mathbf{A}_k^*, \mathbf{A}). \quad (2.30)$$

Com essas relações e com a definição de produto interno dada na equação (2.28), obtém-se as relações de Bose indicadas por

$$[\hat{a}_k, \hat{a}_{k'}^\dagger] = \delta_{kk'}, \quad [\hat{a}_k, \hat{a}_{k'}] = 0. \quad (2.31)$$

Pode-se observar que para modos distintos, os operadores \hat{a}_k e $\hat{a}_{k'}^\dagger$ comutam. Dessa forma, modos distintos representam sistemas quânticos distintos. Para um mesmo modo, os operadores \hat{a}_k e \hat{a}_k^\dagger determinam um espaço de Hilbert individual, sendo o espaço de Hilbert total o produto tensorial dos espaços de Hilbert de todos os modos.

2.2.2 Modos Monocromáticos

Um caso especial da expansão em modos normais ocorre quando esses modos oscilam em uma única frequência, ou seja, os modos são do tipo

$$\mathbf{A}_k(\mathbf{r}, t) = \mathbf{A}_k(\mathbf{r}) \exp(-i\omega_k t). \quad (2.32)$$

Para esse tipo de modo, o produto interno definido pela equação (2.28) é simplificado para

$$(\mathbf{A}_1, \mathbf{A}_2) = \frac{2\varepsilon_0\omega_k}{\hbar} \int \mathbf{A}_1^* \cdot \mathbf{A}_2 \varepsilon dV. \quad (2.33)$$

Com as devidas manipulações, o Hamiltoniano do campo dado pela equação (2.26) é equivalente a

$$\hat{H} = \frac{1}{2} \int \left(\hat{\mathbf{E}} \cdot \hat{\mathbf{D}} + \hat{\mathbf{A}} \cdot \frac{\partial \hat{\mathbf{D}}}{\partial t} \right) dV. \quad (2.34)$$

Uma expressão para \hat{H} em função de \hat{a} e \hat{a}^\dagger é obtida através da substituição das equações (2.18) e (2.20) em (2.34), seguido da expansão em modos normais e aplicação das condições de normalização (2.29) usando (2.33) [36]. Dessa forma, o Hamiltoniano pode ser representado por:

$$\hat{H} = \sum_k \frac{\hbar\omega_k}{2} \left(\hat{a}_k \hat{a}_k^\dagger + \hat{a}_k^\dagger \hat{a}_k \right) = \sum_k \hbar\omega_k \left(\hat{a}_k^\dagger \hat{a}_k + \frac{1}{2} \right). \quad (2.35)$$

Sendo a última identidade obtida a partir das relações de comutação de Bose (2.31).

2.2.3 Operadores do Campo

Na expansão em modos dada em (2.27), as propriedades quânticas estão representadas nos operadores de campo \hat{a}_k e \hat{a}_k^\dagger . Contudo, esses operadores não são hermitianos e, portanto não representam observáveis. Ainda assim, é possível derivar a partir desses dois operadores fundamentais outros operadores que são hermitianos e podem assim ser medidos. No restante desta subseção, as definições estão restritas a um único modo identificado por k .

Os operadores de quadratura \hat{x}_k e \hat{p}_k são definidos a partir de \hat{a}_k e \hat{a}_k^\dagger da seguinte maneira [42]:

$$\hat{x}_k \equiv \sqrt{N_0}(\hat{a}_k + \hat{a}_k^\dagger), \quad \hat{p}_k \equiv -i\sqrt{N_0}(\hat{a}_k - \hat{a}_k^\dagger). \quad (2.36)$$

Nessa definição geral, N_0 representa uma constante real positiva. Em outras notações existentes na literatura, são utilizados os valores $(1/4, 1/2, 1)$ para N_0 . Como pode ser verificado, os operadores de quadratura são hermitianos. A relação de comutação entre \hat{x}_k e \hat{p}_k deriva das relações de comutação de Bose (2.31) e são dadas por:

$$[\hat{x}_k, \hat{p}_k] = i2N_0[\hat{a}_k, \hat{a}_k^\dagger] = i2N_0. \quad (2.37)$$

Essa relação de comutação é similar à encontrada para os operadores de posição e momentum definidos para um oscilador harmônico, que vale $i\hbar$. Por essa razão, diz-se que os operadores de quadratura se comportam como operadores de posição e momentum. A partir da relação de comutação (2.37) e do princípio da incerteza de Heisenberg (2.9), tem-se que:

$$(\Delta\hat{x}_k)(\Delta\hat{p}_k) \geq N_0. \quad (2.38)$$

A partir da equação que relaciona o campo elétrico com o potencial vetor (2.20), é possível obter um operador campo elétrico $\hat{\mathbf{E}}$. O operador campo elétrico é dado por [42]

$$\hat{\mathbf{E}}_k = iE_0\{\hat{a}_k \exp[i(\mathbf{k} \cdot \mathbf{r} - \omega_k t)] - \hat{a}_k^\dagger \exp[-i(\mathbf{k} \cdot \mathbf{r} - \omega_k t)]\}\mathbf{u}_k, \quad (2.39)$$

em que E_0 contém todos os fatores dimensionais, \mathbf{k} representa o vetor de onda e \mathbf{u}_k , um vetor unitário que indica a direção de polarização. Pode-se também representar $\hat{\mathbf{E}}_k$ em função dos operadores de quadratura, de modo que:

$$\hat{\mathbf{E}}_k = -\frac{E_0}{\sqrt{N_0}}[\hat{x}_k \sin(\mathbf{k} \cdot \mathbf{r} - \omega_k t) + \hat{p}_k \cos(\mathbf{k} \cdot \mathbf{r} - \omega_k t)]\mathbf{u}_k. \quad (2.40)$$

Dessa forma, pode-se notar que os operadores \hat{x}_k e \hat{p}_k atuam como componentes de quadratura do operador campo elétrico.

Outro operador de grande relevância é o Hamiltoniano \hat{H} , que já foi previamente derivado na equação (2.35). Este operador representa a energia do sistema. Para um único modo, o Hamiltoniano se reduz a

$$\hat{H} = \hbar\omega_k \left(\hat{a}_k^\dagger \hat{a}_k + \frac{1}{2} \right). \quad (2.41)$$

Pode-se observar que \hat{H} é proporcional a $\hat{a}_k^\dagger \hat{a}_k$, sendo esta quantidade definida como o operador número ($\hat{n} \equiv \hat{a}_k^\dagger \hat{a}_k$). Esse operador permite obter o número de fótons em um determinado modo.

2.3 Estados do Campo Eletromagnético

Foi mostrado anteriormente que as amplitudes \hat{a}_k dos modos do campo são responsáveis pelos efeitos quânticos observados no campo eletromagnético. Entretanto, para que sejam calculadas médias e flutuações (desvio padrão) de quantidades observáveis, descritas por operadores hermitianos, é necessário especificar os estados quânticos do campo. Na sequência, alguns desses estados são descritos e analisados.

2.3.1 Estados de Quadratura

Os estados de quadratura denotados por $|x\rangle$ e $|p\rangle$ são autoestados dos operadores de quadraturas definidos na equação (2.36). Tem-se então que

$$\hat{x}|x\rangle = x|x\rangle, \quad \hat{p}|p\rangle = p|p\rangle, \quad (2.42)$$

em que $x \in \mathbb{R}$ e $p \in \mathbb{R}$ são os autovalores correspondentes aos autoestados $|x\rangle$ e $|p\rangle$, respectivamente. Como x e p são contínuos, diz-se que os operadores de quadratura são observáveis com espectro contínuo. Além disso, os autoestados $|x\rangle$ e $|p\rangle$ são ortogonais,

$$\langle x|x'\rangle = \delta(x - x'), \quad \langle p|p'\rangle = \delta(p - p') \quad (2.43)$$

e completos,

$$\int_{-\infty}^{\infty} |x\rangle \langle x| dx = \mathbb{I}, \quad \int_{-\infty}^{\infty} |p\rangle \langle p| dp = \mathbb{I}. \quad (2.44)$$

Os autoestados de quadratura estão relacionados através da transformada de Fourier, de modo que

$$|x\rangle = \frac{1}{\sqrt{4\pi N_0}} \int_{-\infty}^{\infty} \exp\left(-\frac{ipx}{2N_0}\right) |p\rangle dp, \quad (2.45)$$

$$|p\rangle = \frac{1}{\sqrt{4\pi N_0}} \int_{-\infty}^{\infty} \exp\left(\frac{ipx}{2N_0}\right) |x\rangle dx. \quad (2.46)$$

Conforme mencionado anteriormente, além da notação utilizada aqui para os operadores de quadratura, existem outras convenções utilizadas na literatura. Essas notações são identificadas pelo fator que multiplica a unidade imaginária no comutador (2.37). Na tabela 2.1, são mostradas as relações entre os operadores de quadratura para diferentes convenções encontradas na literatura.

Tabela 2.1 Diferentes representações para os operadores de quadratura do campo.

Notação	$\hbar = 1/2$ ($N_0 = 1/4$)	$\hbar = 1$ ($N_0 = 1/2$)	$\hbar = 2$ ($N_0 = 1$)
Quadraturas	$\hat{x} = \frac{1}{2}(\hat{a} + \hat{a}^\dagger)$ $\hat{p} = -\frac{i}{2}(\hat{a} - \hat{a}^\dagger)$ $\hat{a} = \hat{x} + i\hat{p}$	$\hat{x} = \frac{1}{\sqrt{2}}(\hat{a} + \hat{a}^\dagger)$ $\hat{p} = -\frac{i}{\sqrt{2}}(\hat{a} - \hat{a}^\dagger)$ $\hat{a} = \frac{1}{\sqrt{2}}(\hat{x} + i\hat{p})$	$\hat{x} = \hat{a} + \hat{a}^\dagger$ $\hat{p} = -i(\hat{a} - \hat{a}^\dagger)$ $\hat{a} = \frac{1}{2}(\hat{x} + i\hat{p})$
$[\hat{x}, \hat{p}]$	$\frac{i}{2}$	i	$2i$
$\Delta x \Delta p$	$\frac{1}{4}$	$\frac{1}{2}$	1

2.3.2 Estados de Fock

Os estados de Fock ou estados número são os autoestados do operador número $\hat{n} = \hat{a}^\dagger \hat{a}$, ou seja,

$$\hat{n} |n\rangle = n |n\rangle, \quad (2.47)$$

sendo n um inteiro não negativo que representa o número de fótons no modo eletromagnético.

Algumas propriedades dos estados número merecem ser destacadas. Os estados número são autoestados do Hamiltoniano (2.41), ou seja,

$$\hat{H} |n\rangle = \hbar\omega \left(\hat{a}^\dagger \hat{a} + \frac{1}{2} \right) |n\rangle = \hbar\omega \left(\hat{n} + \frac{1}{2} \right) |n\rangle = \hbar\omega \left(n + \frac{1}{2} \right) |n\rangle = E_n |n\rangle, \quad (2.48)$$

sendo E_n a energia no modo. Como consequência disso, os estados número formam uma base ortonormal e completa que é também conhecida como base de Fock. A ação dos operadores \hat{a} e \hat{a}^\dagger sobre os estados número é representada por:

$$\hat{a} |n\rangle = \sqrt{n} |n-1\rangle, \quad (2.49)$$

$$\hat{a}^\dagger |n\rangle = \sqrt{n+1} |n+1\rangle. \quad (2.50)$$

Observa-se que \hat{a} diminui em uma unidade o número de fótons do modo. Dessa forma, ele é conhecido como operador de aniquilação ou de destruição. Por outro lado, o operador \hat{a}^\dagger aumenta o número de fótons e por isso ele é conhecido como operador de criação. Como consequência das equações (2.49) e (2.50), tem-se que:

$$\hat{a} |0\rangle = 0, \quad \langle 0 | \hat{a}^\dagger = 0, \quad (2.51)$$

$$|n\rangle = \frac{1}{\sqrt{n!}} (\hat{a}^\dagger)^n |0\rangle. \quad (2.52)$$

O estado $|0\rangle$ é chamado de estado vácuo (*vacuum state*). Apesar de não possuir fótons, o vácuo possui flutuações que podem ser medidas, como pode ser observado para os seguintes operadores:

$$\langle \hat{x} \rangle_0 = \langle 0 | \hat{x} | 0 \rangle = \sqrt{N_0} \langle 0 | (\hat{a}^\dagger + \hat{a}) | 0 \rangle = 0, \quad (2.53)$$

$$\langle \hat{p} \rangle_0 = \langle 0 | \hat{p} | 0 \rangle = -i\sqrt{N_0} \langle 0 | (\hat{a}^\dagger - \hat{a}) | 0 \rangle = 0, \quad (2.54)$$

$$\langle \hat{\mathbf{E}}_k \rangle_0 = -\frac{E_0}{\sqrt{N_0}} [\langle \hat{x} \rangle_{|0\rangle} \sin(\mathbf{k} \cdot \mathbf{r} - \omega_k t) + \langle \hat{p} \rangle_{|0\rangle} \cos(\mathbf{k} \cdot \mathbf{r} - \omega_k t)] = 0, \quad (2.55)$$

$$\langle \hat{x}^2 \rangle_0 = N_0 \langle 0 | (\hat{a}^\dagger + \hat{a})^2 | 0 \rangle = N_0 \langle 0 | (\hat{a}^\dagger \hat{a}^\dagger + 2\hat{a}^\dagger \hat{a} + \hat{a} \hat{a} + 1) | 0 \rangle = N_0, \quad (2.56)$$

$$\langle \hat{p}^2 \rangle_0 = -N_0 \langle 0 | (\hat{a}^\dagger - \hat{a})^2 | 0 \rangle = -N_0 \langle 0 | (\hat{a}^\dagger \hat{a}^\dagger - 2\hat{a}^\dagger \hat{a} + \hat{a} \hat{a} - 1) | 0 \rangle = N_0, \quad (2.57)$$

$$\langle \hat{\mathbf{E}}_k^2 \rangle_0 = E_0^2 \langle 0 | (1 + 2\hat{a}^\dagger \hat{a} - \hat{a}^2 e^{2i(\mathbf{k} \cdot \mathbf{r} - \omega_k t)} - (\hat{a}^\dagger)^2 e^{-2i(\mathbf{k} \cdot \mathbf{r} - \omega_k t)}) | 0 \rangle = E_0^2 \quad (2.58)$$

$$(\Delta \hat{x})_0 = \sqrt{\langle \hat{x}^2 \rangle_0 - \langle \hat{x} \rangle_0^2} = \sqrt{N_0}, \quad (2.59)$$

$$(\Delta \hat{p})_0 = \sqrt{\langle \hat{p}^2 \rangle_0 - \langle \hat{p} \rangle_0^2} = \sqrt{N_0}, \quad (2.60)$$

$$(\Delta \hat{\mathbf{E}}_k)_0 = \sqrt{\langle \hat{\mathbf{E}}_k^2 \rangle_0 - \langle \hat{\mathbf{E}}_k \rangle_0^2} = E_0. \quad (2.61)$$

Em (2.56-2.58), foi usada a relação de comutação de Bose e a relação (2.51). Pode-se observar através das equações (2.59) e (2.60) que o vácuo satura a relação de incerteza (2.38) para as quadraturas \hat{x} e \hat{p} . Por isso, o vácuo é dito ser um estado de incerteza mínima. Na Figura 2.1, as flutuações do vácuo são ilustradas através da medição do operador de quadratura \hat{x} , além do histograma obtido com os resultados medidos. É também usual representar as flutuações das quadraturas através de um diagrama como o da Figura 2.2. Nele, o vácuo é representado como um círculo com diâmetro $\sqrt{N_0}$.

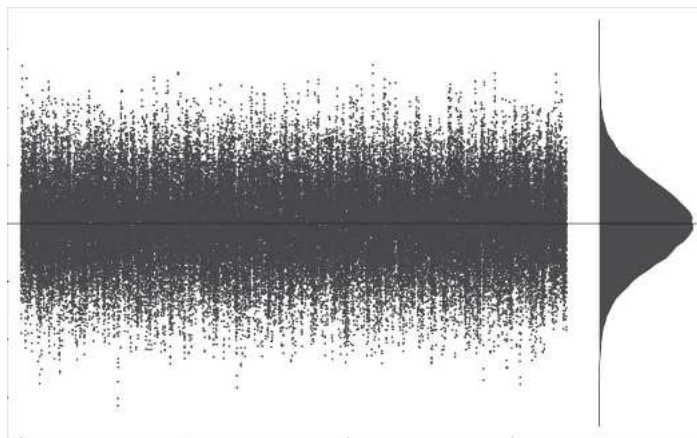


Figura 2.1 Medida da quadratura \hat{x} usando detecção homódina ao longo da escala de tempo. O histograma dos dados é mostrado do lado direito (Figura obtida de [36]).

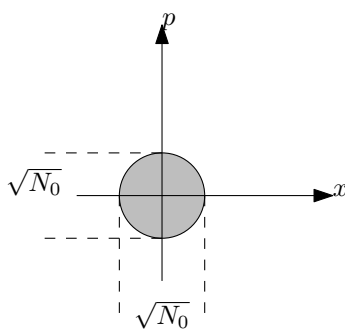


Figura 2.2 Representação das quadraturas do vácuo. O círculo indica que as flutuações de \hat{x} e \hat{p} são idênticas.

2.3.3 Estados Coerentes

Os estados coerentes são o equivalente quântico mais próximo de uma onda eletromagnética clássica. Esses estados, denotados por $|\alpha\rangle$ ($\alpha \in \mathbb{C}$), descrevem o campo proveniente de um laser ideal. De acordo com [41], o campo de um laser monomodo pode ser representado pelo operador densidade

$$\hat{\rho}_F(t) = \int \phi(\alpha, t) |\alpha\rangle \langle \alpha| d^2\alpha, \quad (2.62)$$

em que a integral é calculada sobre todo o plano complexo. A função $\phi(\alpha, t)$ é uma função de ponderação que depende do tipo do laser. No regime contínuo do laser, quando o parâmetro de bombeio óptico aumenta (bem acima do limiar de oscilação), a função $\phi(\alpha, t)$ se aproxima de uma função δ e, dessa forma, o estado do laser pode ser aproximado por um estado coerente. Ou, de forma mais precisa, o estado do laser tende para uma mistura de estados coerentes com fases aleatórias.

Como a luz de um laser possui uma amplitude bem definida, os estados coerentes são definidos como autoestados do operador de amplitude do campo \hat{a} , o operador de aniquilação, ou seja:

$$\hat{a} |\alpha\rangle = \alpha |\alpha\rangle. \quad (2.63)$$

Como \hat{a} não é hermitiano, os autovalores α são números complexos, que correspondem às amplitudes de onda complexas encontradas na óptica clássica.

Os estados coerentes podem ser representados na base de Fock, de modo que:

$$|\alpha\rangle = \exp(-|\alpha|^2/2) \sum_{n=0}^{\infty} \frac{\alpha^n}{(n!)^{1/2}} |n\rangle. \quad (2.64)$$

A partir dessa representação, pode-se obter a distribuição de probabilidade do número de fótons em um estado coerente $|\alpha\rangle$. Esta distribuição é de Poisson e é dada por:

$$p_n = |\langle n|\alpha\rangle|^2 = \frac{|\alpha|^{2n}}{n!} \exp(-|\alpha|^2). \quad (2.65)$$

A quantidade $|\alpha|^2$ equivale ao número médio de fótons em $|\alpha\rangle$, já que $\langle \hat{n} \rangle_\alpha = \langle \alpha | \hat{n} | \alpha \rangle = \langle \alpha | \hat{a}^\dagger \hat{a} | \alpha \rangle = |\alpha|^2$.

Dois estados coerentes $|\alpha\rangle$ e $|\beta\rangle$ quaisquer são não ortogonais, como pode ser verificado através das relações:

$$\langle \alpha | \beta \rangle = \exp\left(-\frac{|\alpha|^2}{2} - \frac{|\beta|^2}{2} + \alpha^* \beta\right), \quad (2.66)$$

$$|\langle \alpha | \beta \rangle|^2 = \exp(-|\alpha - \beta|^2). \quad (2.67)$$

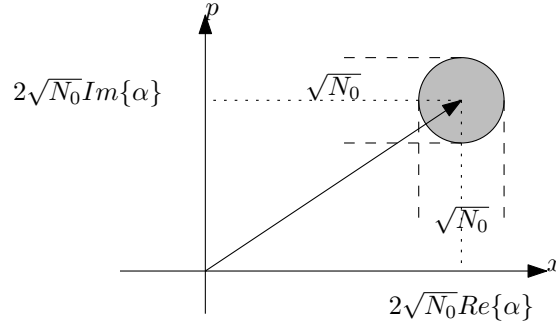


Figura 2.3 Representação das quadraturas de um estado coerente $|\alpha\rangle$. Um estado coerente pode ser interpretado como o vácuo deslocado.

Em relação às flutuações, os estados coerentes verificam as seguintes relações:

$$\langle \hat{x} \rangle_\alpha = \sqrt{N_0} \langle \alpha | (\hat{a} + \hat{a}^\dagger) | \alpha \rangle = \sqrt{N_0} (\alpha + \alpha^*) = 2\sqrt{N_0} \Re\{\alpha\}, \quad (2.68)$$

$$\langle \hat{p} \rangle_\alpha = -i\sqrt{N_0} \langle \alpha | (\hat{a} - \hat{a}^\dagger) | \alpha \rangle = -i\sqrt{N_0} (\alpha - \alpha^*) = 2\sqrt{N_0} \Im\{\alpha\}, \quad (2.69)$$

$$\begin{aligned} \langle \hat{\mathbf{E}}_k \rangle_\alpha &= iE_0 (\alpha e^{i(\mathbf{k}\cdot\mathbf{r}-\omega_k t)} - \alpha^* e^{-i(\mathbf{k}\cdot\mathbf{r}-\omega_k t)}) \mathbf{u}_k \\ &= -\frac{2E_0}{\sqrt{N_0}} [\Re\{\alpha\} \sin(\mathbf{k}\cdot\mathbf{r} - \omega_k t) + \Im\{\alpha\} \cos(\mathbf{k}\cdot\mathbf{r} - \omega_k t)] \mathbf{u}_k, \end{aligned} \quad (2.70)$$

$$\langle \hat{x}^2 \rangle_\alpha = N_0 \langle \alpha | (\hat{a} + \hat{a}^\dagger)^2 | \alpha \rangle = N_0 [1 + (\alpha + \alpha^*)^2], \quad (2.71)$$

$$\langle \hat{p}^2 \rangle_\alpha = -N_0 \langle \alpha | (\hat{a} - \hat{a}^\dagger)^2 | \alpha \rangle = N_0 [1 - (\alpha - \alpha^*)^2], \quad (2.72)$$

$$\langle \hat{\mathbf{E}}_k^2 \rangle_\alpha = E_0^2 [1 - (\alpha e^{i(\mathbf{k}\cdot\mathbf{r}-\omega_k t)} - \alpha^* e^{-i(\mathbf{k}\cdot\mathbf{r}-\omega_k t)})^2], \quad (2.73)$$

$$(\Delta \hat{x})_\alpha = \sqrt{\langle \hat{x}^2 \rangle_\alpha - \langle \hat{x} \rangle_\alpha^2} = \sqrt{N_0}, \quad (2.74)$$

$$(\Delta \hat{p})_\alpha = \sqrt{\langle \hat{p}^2 \rangle_\alpha - \langle \hat{p} \rangle_\alpha^2} = \sqrt{N_0}, \quad (2.75)$$

$$(\Delta \hat{\mathbf{E}}_k)_\alpha = \sqrt{\langle \hat{\mathbf{E}}_k^2 \rangle_\alpha - \langle \hat{\mathbf{E}}_k \rangle_\alpha^2} = E_0. \quad (2.76)$$

A partir dessas relações, pode-se observar que os operadores de quadratura e do campo elétrico possuem as mesmas flutuações que o vácuo. Além disso, o valor médio do campo elétrico é equivalente a uma onda eletromagnética clássica. Pode-se verificar também que, do mesmo modo que o vácuo, os estados coerentes são estados de incerteza mínima para as quadraturas \hat{x} e \hat{p} . Na Figura 2.3 tem-se a representação gráfica para as quadraturas de um estado coerente $|\alpha\rangle$. Pode-se observar que um estado coerente pode ser interpretado como um vácuo deslocado.

2.3.4 Estados Comprimidos

Tanto os estados coerentes como o vácuo possuem flutuações iguais para as quadraturas x e p , além de serem estados de incerteza mínima de acordo com (2.38). Quando são explorados efeitos ópticos não lineares, como no caso da amplificação óptica paramétrica degenerada e não degenerada, é possível produzir estados cujas flutuações em uma determinada quadratura são inferiores a $\sqrt{N_0}$. Esses estados são conhecidos como estados comprimidos (*squeezed states*).

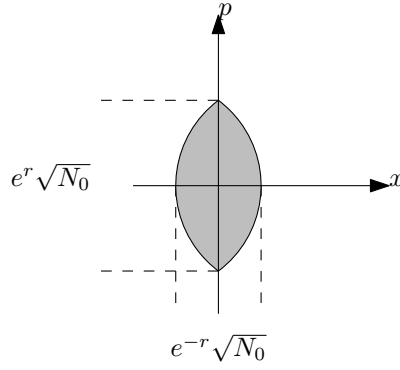


Figura 2.4 Representação das quadraturas do vácuo comprimido. Nesse caso, a quadratura x é comprimida enquanto que a quadratura p é expandida.

Considerando o caso de um amplificador óptico paramétrico degenerado com fator de compressão r , que tem como entrada um modo de vácuo com operadores de quadratura denotados por $\hat{x}^{(0)}$ e $\hat{p}^{(0)}$. O modo de saída do amplificador tem as suas quadraturas dadas por:

$$\hat{x}(r) = e^{-r}\hat{x}^{(0)}, \quad \hat{p}(r) = e^r\hat{p}^{(0)}. \quad (2.77)$$

Quando $r > 0$, a quadratura x é comprimida enquanto que a quadratura p é expandida. Quando $r < 0$, os papéis são invertidos. As flutuações do vácuo comprimido são dadas por:

$$\Delta\hat{x}(r) = e^{-r}\sqrt{N_0}, \quad \Delta\hat{p}(r) = e^r\sqrt{N_0}. \quad (2.78)$$

Pode-se notar que o vácuo comprimido ainda é um estado de incerteza mínima. Na Figura 2.4, tem-se uma ilustração das quadraturas para o vácuo comprimido. Além do vácuo, podem-se comprimir também as quadraturas de estados coerentes.

Se um amplificador óptico paramétrico não degenerado é utilizado, são produzidos dois modos de saída que são correlacionados. O estado resultante é denominado de estado comprimido bimodal e representa um exemplo de estado emaranhado. As quadraturas de um estado comprimido bimodal podem ser escritas como:

$$\hat{x}_1 = \frac{1}{\sqrt{2}}(e^r\hat{x}_1^{(0)} + e^{-r}\hat{x}_2^{(0)}), \quad \hat{p}_1 = \frac{1}{\sqrt{2}}(e^{-r}\hat{p}_1^{(0)} + e^r\hat{p}_2^{(0)}), \quad (2.79)$$

$$\hat{x}_2 = \frac{1}{\sqrt{2}}(e^r\hat{x}_1^{(0)} - e^{-r}\hat{x}_2^{(0)}), \quad \hat{p}_2 = \frac{1}{\sqrt{2}}(e^{-r}\hat{p}_1^{(0)} - e^r\hat{p}_2^{(0)}). \quad (2.80)$$

Para esses modos, tem-se que:

$$\hat{x}_1 - \hat{x}_2 = \sqrt{2}e^{-r}\hat{x}_2^{(0)}, \quad \langle(\hat{x}_1 - \hat{x}_2)^2\rangle = 2N_0e^{-2r}, \quad (2.81)$$

$$\hat{p}_1 + \hat{p}_2 = \sqrt{2}e^{-r}\hat{p}_1^{(0)}, \quad \langle(\hat{p}_1 + \hat{p}_2)^2\rangle = 2N_0e^{-2r}. \quad (2.82)$$

Assim, no limite quando $r \rightarrow \infty$, $\hat{x}_1 \rightarrow \hat{x}_2$ e $\hat{p}_1 \rightarrow -\hat{p}_2$.

2.4 Representações no Espaço de Fase

Na seção 2.1, destacou-se o fato de que para se obter as estatísticas de um sistema quântico é necessário que o mesmo seja descrito por um vetor de estados ou, de forma mais geral, por um operador densidade. Na óptica quântica, entretanto, é mais conveniente usar uma formulação equivalente em termos de funções de quasiprobabilidade. As funções principais são a Q, a P e a de Wigner [46]. Elas recebem a denominação de funções de quasiprobabilidade, pois podem assumir valores negativos ao longo de seu domínio, ao contrário de uma verdadeira distribuição de probabilidade que é estritamente não negativa. Para os estados quânticos considerados nesta tese, a caracterização por meio da função de Wigner é suficiente. A função de Wigner é definida sobre um espaço real simplético¹ (espaço de fase). A formulação descrita nesta seção utiliza os resultados apresentados em [16].

Um sistema quântico é dito ser um sistema de variáveis contínuas se ele possui um espaço de Hilbert de dimensão infinita descrito por observáveis com espectro contínuo. Formalmente, um sistema de variáveis contínuas é representado por N modos bosônicos², correspondendo aos N modos de radiação quantizada do campo eletromagnético. O espaço de Hilbert de dimensão infinita é representado por

$$\mathcal{H} = \bigotimes_{k=1}^N \mathcal{H}_k, \quad (2.83)$$

que representa o produto tensorial de N espaços de Fock \mathcal{H}_k (espaço expandido pela base de Fock). Aos N modos bosônicos estão associados N pares de operadores de aniquilação e criação $\{\hat{a}_k, \hat{a}_k^\dagger\}_{k=1}^N$, cujas relações de comutação verificam

$$[\hat{a}_i, \hat{a}_j] = 0, \quad [\hat{a}_i^\dagger, \hat{a}_j^\dagger] = 0, \quad [\hat{a}_i, \hat{a}_j^\dagger] = -[\hat{a}_j^\dagger, \hat{a}_i] = \delta_{i,j}. \quad (2.84)$$

Os operadores de campo $\{\hat{a}_k, \hat{a}_k^\dagger\}_{k=1}^N$ podem ser agrupados em um vetor $\hat{\mathbf{b}}$, tal que

$$\hat{\mathbf{b}} = (\hat{a}_1, \hat{a}_1^\dagger, \dots, \hat{a}_N, \hat{a}_N^\dagger), \quad (2.85)$$

$$[\hat{b}_i, \hat{b}_j] = \Omega_{ij} \quad (i, j = 1, \dots, 2N), \quad (2.86)$$

sendo Ω_{ij} um elemento genérico da matriz antissimétrica de dimensão $2N \times 2N$ definida por

$$\Omega = \bigoplus_{k=1}^N \omega = \begin{pmatrix} \omega & & \\ & \ddots & \\ & & \omega \end{pmatrix}, \quad \omega = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}. \quad (2.87)$$

¹Seja V um espaço vetorial real e $\Omega : V \times V \rightarrow \mathbb{R}$, uma forma bilinear antissimétrica. Diz-se que a forma Ω é não degenerada ou simplética se $\Omega(\mathbf{u}, \mathbf{v}) = 0 \quad \forall \mathbf{v} \in V \implies \mathbf{u} = 0$. Nesse caso, o par (V, Ω) é um espaço vetorial simplético. Para uma matriz antissimétrica A , $\Omega(\mathbf{u}, \mathbf{v}) = \mathbf{u}' A \mathbf{v}$. [47]

²Fótons são classificados como bósons - partículas com *spin* inteiro.

Os N pares de operadores de quadratura $\{\hat{x}_k, \hat{p}_k\}_{k=1}^N$ podem ser dispostos no vetor

$$\hat{\mathbf{v}} = (\hat{x}_1, \hat{p}_1, \dots, \hat{x}_N, \hat{p}_N)^T, \quad (2.88)$$

de modo que,

$$\hat{\mathbf{v}}^T |\mathbf{v}\rangle = \mathbf{v}^T |\mathbf{v}\rangle, \quad (2.89)$$

em que $\mathbf{v} \in \mathbb{R}^{2N}$ e $|\mathbf{v}\rangle = (|v_1\rangle, \dots, |v_{2N}\rangle)^T$.

2.4.1 Função de Wigner

A função de Wigner pode ser formulada de diversas maneiras equivalentes. Neste texto, será apresentada a formulação baseada nas quadraturas do campo. Inicialmente, serão mostradas as equações para N modos, assim como descrito em [16]. Em seguida, serão mostradas formas mais específicas envolvendo um modo único, como descrito em [36].

Seja $\hat{\rho} : \mathcal{H}^{\otimes N} \rightarrow \mathcal{H}^{\otimes N}$, o operador densidade do sistema bosônico de N modos. O operador de Weyl é definido como

$$D(\xi) \triangleq \exp(i\hat{\mathbf{v}}^T \boldsymbol{\Omega} \xi), \quad (2.90)$$

em que $\xi \in \mathbb{R}^{2N}$. Então, um $\hat{\rho}$ arbitrário é equivalente a uma função característica de Wigner definida por

$$\chi(\xi) \triangleq \text{Tr}[\hat{\rho} D(\xi)], \quad (2.91)$$

em que $\text{Tr}[\cdot]$ representa o traço. A equação (2.91) representa o valor esperado do operador de Weyl $D(\xi)$ em um sistema quântico descrito pelo operador densidade $\hat{\rho}$. A função de Wigner é obtida a partir da transformada de Fourier da função característica de Wigner e é denotada por

$$W(\mathbf{v}) = \int_{\mathbb{R}^{2N}} \frac{d^{2N}\xi}{(2\pi)^{2N}} \exp(-i\mathbf{v}^T \boldsymbol{\Omega} \xi) \chi(\xi), \quad (2.92)$$

que é normalizada à unidade. Na definição de $W(\mathbf{v})$, \mathbf{v} corresponde aos autovalores dos operadores de quadratura, assim como na equação (2.89). Essas variáveis expandem um espaço real simplético $\mathcal{K} = (\mathbb{R}^{2N}, \boldsymbol{\Omega})$, que é chamado de espaço de fase. Dessa forma, um estado quântico arbitrário $\hat{\rho}$ de um sistema bosônico de N modos é equivalente a uma função de Wigner $W(\mathbf{v})$ definida sobre um espaço de fase \mathcal{K} de dimensão $2N$ [16].

Para um estado quântico $\hat{\rho}$, os momentos estatísticos média ($\bar{\mathbf{v}}$) e covariância (\mathbf{V}) são dados por

$$\bar{\mathbf{v}} = \text{Tr}(\hat{\mathbf{v}}\hat{\rho}), \quad (2.93)$$

$$\mathbf{V}_{(2N \times 2N)} : V_{ij} = \frac{1}{2} \langle \{\Delta\hat{v}_i, \Delta\hat{v}_j\} \rangle = \frac{1}{2} \langle \Delta\hat{v}_i \Delta\hat{v}_j + \Delta\hat{v}_j \Delta\hat{v}_i \rangle, \quad (2.94)$$

com $\Delta\hat{v}_i = \hat{v}_i - \langle \hat{v}_i \rangle$. A notação $\{A, B\} = AB + BA$ corresponde ao anticomutador. Na diagonal de \mathbf{V} estão representadas as variâncias dos operadores de quadratura, ou seja, os elementos $V_{ii} = V(\hat{v}_i) = \langle (\Delta\hat{v}_i)^2 \rangle = \langle \hat{v}_i^2 \rangle - \langle \hat{v}_i \rangle^2$. A matriz de covariância \mathbf{V} é uma matriz real e simétrica que deve satisfazer a relação

$$\mathbf{V} + i\boldsymbol{\Omega} \geq 0. \quad (2.95)$$

Com a média e a covariância é possível caracterizar completamente os estados denominados de estados gaussianos³. Para esses estados, as representações de Wigner são gaussianas, com expressões dadas por:

$$\chi(\xi) = \exp \left[-\frac{1}{2} \xi^T (\boldsymbol{\Omega} \mathbf{V} \boldsymbol{\Omega}^T) \xi - i(\boldsymbol{\Omega} \bar{\mathbf{v}})^T \xi \right], \quad (2.96)$$

$$W(\mathbf{x}) = \frac{\exp \left[-(1/2)(\mathbf{v} - \bar{\mathbf{v}})^T \mathbf{V}^{-1} (\mathbf{v} - \bar{\mathbf{v}}) \right]}{(2\pi)^N \sqrt{\det \mathbf{V}}}. \quad (2.97)$$

Cabe ressaltar que as equações (2.92), (2.96) e (2.97) estão escritas na notação $\hbar = 2$ (Tabela 2.1).

Para um único modo, com a notação $\hbar = 1$, e considerando-se as quadraturas x e p , a função de Wigner pode ser representada como [36]

$$W(x, p) = \frac{1}{2\pi} \int_{-\infty}^{\infty} \exp(i p y) \left\langle x - \frac{y}{2} \left| \hat{\rho} \right| x + \frac{y}{2} \right\rangle dy. \quad (2.98)$$

De modo similar, a função característica de Wigner pode ser representada como

$$\chi(u, z) = \int_{-\infty}^{\infty} \exp(-i u y) \left\langle y - \frac{z}{2} \left| \hat{\rho} \right| y + \frac{z}{2} \right\rangle dy. \quad (2.99)$$

Apesar de não ser uma distribuição de probabilidade genuína, a função de Wigner resulta em distribuições genuínas para medições homódinas. No caso de N modos descritos por uma função de Wigner $W(x_1, p_1, \dots, x_N, p_N)$, a distribuição conjunta dos resultados das N medições

³Os estados coerentes, comprimidos e o vácuo são exemplos de estados gaussianos.

homódinas (uma quadratura medida por modo) é obtida através da integração da função de Wigner sobre as quadraturas não medidas. Como exemplos de distribuições, tem-se:

$$\Pr(x_1, p_2) = \int_{-\infty}^{\infty} \int_{-\infty}^{\infty} dx_2 dp_1 W(x_1, p_1, x_2, p_2), \quad (2.100)$$

$$\Pr(x) = \langle x | \hat{\rho} | x \rangle = \int_{-\infty}^{\infty} dp W(x, p), \quad (2.101)$$

$$\Pr(p) = \langle p | \hat{\rho} | p \rangle = \int_{-\infty}^{\infty} dx W(x, p). \quad (2.102)$$

As duas últimas equações representam casos especiais de uma rotação de um ângulo θ no espaço de fases ($\theta = 0$ na equação (2.101) e $\theta = \pi/2$ na equação (2.102)) conhecida como transformação de Radon e dada por:

$$\begin{aligned} \Pr(x, \theta) &= \langle x | \hat{U}(\theta) \hat{\rho} \hat{U}^\dagger(\theta) | x \rangle \\ &= \int_{-\infty}^{\infty} W(x \cos \theta - p \sin \theta, x \sin \theta + p \cos \theta) dp. \end{aligned} \quad (2.103)$$

Como exemplo de aplicação da equação (2.98), pode-se calcular a função de Wigner para o vácuo $|0\rangle$. Usando o fato de que $\hat{\rho} = |0\rangle \langle 0|$ e

$$\psi_0(x) \equiv \langle x | 0 \rangle = \frac{1}{\sqrt[4]{\pi}} \exp(-x^2/2), \quad (2.104)$$

então

$$\begin{aligned} W_0(x, p) &= \frac{1}{2\pi} \int_{-\infty}^{\infty} \exp(ipy) \psi_0(x - y/2) \psi_0(x + y/2) dy \\ &= \frac{\exp(-x^2)}{2\pi\sqrt{\pi}} \int_{-\infty}^{\infty} \exp(ipy - y^2/4) dy \\ &= \frac{1}{\pi} \exp(-x^2 - p^2). \end{aligned} \quad (2.105)$$

A função $\psi_0(x)$ representa a função de onda do vácuo. O gráfico de $W_0(x, p)$ está ilustrado na Figura 2.5. A função de Wigner dos estados coerentes pode ser obtida facilmente a partir do fato de que um estado coerente corresponde ao vácuo deslocado. Pode-se então mostrar que um estado coerente de amplitude complexa $\alpha = 1/\sqrt{2}(x_0 + ip_0)$ ($\hbar = 1$) possui função de Wigner

$$W_C(x, p) = W_0(x - x_0, p - p_0) = \frac{1}{\pi} \exp[-(x - x_0)^2 - (p - p_0)^2]. \quad (2.106)$$

2.4.2 Operações Gaussianas

Uma operação gaussiana transforma estados gaussianos em estados gaussianos. Essas operações podem envolver a ação de canais quânticos, bem como transformações unitárias

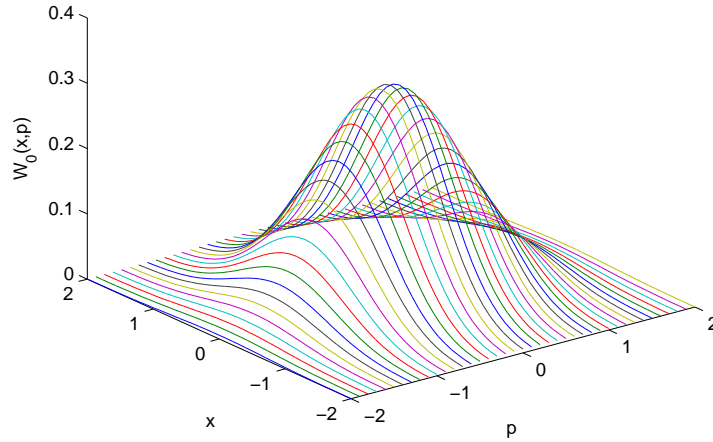


Figura 2.5 Função de Wigner para o vácuo. Nota-se que ela corresponde a uma gaussiana bidimensional.

como as mencionadas na seção 2.1. A ação de uma operação gaussiana nos operadores de quadratura é descrita na representação de Heisenberg pelo mapa afim

$$(\mathbf{S}, \mathbf{d}) : \hat{\mathbf{v}} \rightarrow \mathbf{S}\hat{\mathbf{v}} + \mathbf{d}, \quad (2.107)$$

em que $\mathbf{d} \in \mathbb{R}^{2N}$ e \mathbf{S} é uma matriz $2N \times 2N$. Para que essa operação preserve as relações de comutação dos operadores de quadratura, \mathbf{S} deve ser uma matriz simplética, ou seja:

$$\mathbf{S}\Omega\mathbf{S}^T = \Omega. \quad (2.108)$$

Os autovalores \mathbf{v} dos operadores de quadratura $\hat{\mathbf{v}}$ também satisfazem o mapa afim, ou seja:

$$(\mathbf{S}, \mathbf{d}) : \mathbf{v} \rightarrow \mathbf{S}\mathbf{v} + \mathbf{d}. \quad (2.109)$$

Por fim, os momentos estatísticos $\bar{\mathbf{v}}$ e \mathbf{V} são transformados da seguinte forma:

$$\bar{\mathbf{v}} \rightarrow \mathbf{S}\bar{\mathbf{v}} + \mathbf{d}, \quad \mathbf{V} \rightarrow \mathbf{S}\mathbf{V}\mathbf{S}^T. \quad (2.110)$$

Uma operação gaussiana de grande importância é o divisor de feixe (*Beamsplitter* - BS). O BS é um dispositivo óptico de quatro portas, sendo duas de entrada e duas de saída, assim como ilustrado na Figura 2.6. Os modos de saída são transformados da seguinte forma:

$$\begin{pmatrix} \hat{a}_1 \\ \hat{a}_2 \end{pmatrix} \rightarrow \begin{pmatrix} \sqrt{\tau} & \sqrt{1-\tau} \\ -\sqrt{1-\tau} & \sqrt{\tau} \end{pmatrix} \begin{pmatrix} \hat{a}_1 \\ \hat{a}_2 \end{pmatrix}. \quad (2.111)$$

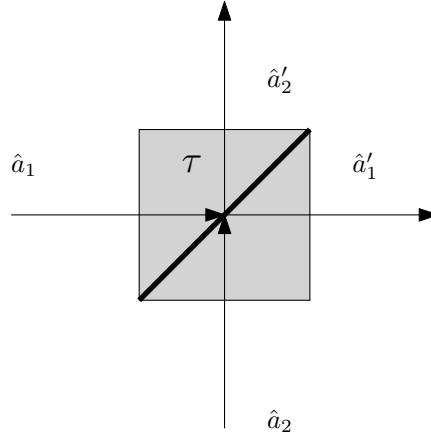


Figura 2.6 Representação de um divisor de feixe (BS) de transmissividade τ . Os modos de entrada \hat{a}_1 e \hat{a}_2 são combinados no BS resultando nos modos de saída \hat{a}'_1 (transmitido) e \hat{a}'_2 (refletido).

Nessa transformação, $\tau \in [0, 1]$ representa a transmissividade do BS. Os operadores de quadratura $\hat{\mathbf{v}} = (\hat{x}_1, \hat{p}_1, \hat{x}_2, \hat{p}_2)^T$ são transformados de acordo com a transformação afim dada por

$$\hat{\mathbf{v}} \rightarrow \mathbf{B}(\tau)\hat{\mathbf{v}}, \quad \mathbf{B}(\tau) = \begin{pmatrix} \sqrt{\tau}\mathbf{I} & \sqrt{1-\tau}\mathbf{I} \\ -\sqrt{1-\tau}\mathbf{I} & \sqrt{\tau}\mathbf{I} \end{pmatrix}, \quad (2.112)$$

em que \mathbf{I} representa a matriz identidade 2×2 .

O BS pode ser usado para modelar as perdas por atenuação em um canal quântico. Para modelar um canal com transmissão T (T corresponde a fração de potência do sinal que é transmitida), considera-se um BS com transmissividade T . As duas entradas correspondem a um modo com quadraturas $(\hat{x}_{in}, \hat{p}_{in})$ e a um modo de vácuo com quadraturas $(\hat{x}_{vac}, \hat{p}_{vac})$. O modo de saída correspondente a parte refletida no BS é descartado, enquanto que as quadraturas do outro modo correspondem a

$$\hat{x}_{out} = \sqrt{T}\hat{x}_{in} + \sqrt{1-T}\hat{x}_{vac} = \sqrt{T}(\hat{x}_{in} + B_x), \quad (2.113)$$

$$\hat{p}_{out} = \sqrt{T}\hat{p}_{in} + \sqrt{1-T}\hat{p}_{vac} = \sqrt{T}(\hat{p}_{in} + B_p), \quad (2.114)$$

$$B_x = \sqrt{\frac{1-T}{T}}\hat{x}_{vac}, \quad B_p = \sqrt{\frac{1-T}{T}}\hat{p}_{vac}, \quad (2.115)$$

$$\langle B_x^2 \rangle = \langle B_p^2 \rangle = \frac{1-T}{T}N_0 = \chi N_0, \quad (2.116)$$

sendo B_x e B_p denominados de ruído equivalente na entrada.

2.4.3 Decomposição de Estados Gaussianos

Na análise de estados gaussianos é conveniente usar formas de decomposição para a matriz de covariância \mathbf{V} , tais como a decomposição de Williamson. De acordo com ela, para

uma matriz de covariância \mathbf{V} arbitrária, referente a N modos, existe uma matriz simplética \mathbf{S} tal que

$$\mathbf{V} = \mathbf{S}\mathbf{V}^\oplus\mathbf{S}^T, \quad \mathbf{V}^\oplus = \bigoplus_{k=1}^N \nu_k \mathbf{I}, \quad (2.117)$$

em que a matriz diagonal \mathbf{V}^\oplus é chamada de forma de Williamson de \mathbf{V} e as N quantidades positivas ν_k são denominadas de autovalores simpléticos de \mathbf{V} . Uma das maneiras de calcular o espectro $\{\nu_k\}_{k=1}^N, \nu_k \geq 1$ é através do cálculo dos autovalores da matriz $|i\Omega\mathbf{V}|$. Os $2N$ autovalores de $|i\Omega\mathbf{V}|$ são obtidos tomando-se o módulo dos $2N$ autovalores reais de $i\Omega\mathbf{V}$. Esses $2N$ autovalores resultam nos N autovalores simpléticos de \mathbf{V} .

A decomposição de Williamson permite que a entropia de von Neumann $S(\hat{\rho})$ para um estado gaussiano $\hat{\rho}$ seja escrita como

$$S(\hat{\rho}) = \sum_{k=1}^N g(\nu_k), \quad (2.118)$$

em que

$$g(x) = \left(\frac{x+1}{2}\right) \log\left(\frac{x+1}{2}\right) - \left(\frac{x-1}{2}\right) \log\left(\frac{x-1}{2}\right). \quad (2.119)$$

Para os estados puros, tem-se que $\nu_k = 1 (k = 1, \dots, N)$, de modo que a entropia $S(\hat{\rho})$ vale zero.

2.5 Medições Ópticas

Como descrito no postulado 2.2, as medidas quânticas são descritas teoricamente por operadores de medição. Esse formalismo engloba tanto as medidas projetivas (também conhecidas como medidas de von Neumann), cujos operadores de medida são projetores como os indicados em (2.5), quanto as medidas generalizadas ou POVM (*positive operator-valued measure*). As medidas POVM são de interesse quando as estatísticas do resultado da medida são mais relevantes que o estado pósmedição. Os operadores POVM são descritos por elementos $\Pi_m \equiv M_m^\dagger M_m$ de modo que $\Pi_m > 0$ e $\sum_m \Pi_m = I$.

Em termos práticos, algumas medidas, tais como a discriminação no número de fótons, ainda representam um desafio tecnológico a ser resolvido. Nessa medida, os operadores de medição são dados por $\{|0\rangle\langle 0|, |1\rangle\langle 1|, \dots, |n\rangle\langle n|, \dots\}$. Em vez disso, é realizada a discriminação entre a presença ou ausência de fótons representada pelos operadores $\{|0\rangle\langle 0|, \mathbb{I} - |0\rangle\langle 0|\}$. Tal operação é realizada com APDs. Para medir os operadores de quadratura de um modo do campo eletromagnético, pode-se utilizar a detecção homódina. Esse tipo de detecção equivale a medir o projetor $|x\rangle\langle x|$ ou o projetor $|p\rangle\langle p|$ [16]. As distribuições das quadraturas medidas são dadas pelas equações (2.101) ou (2.102). A medição simultânea de ambas as quadraturas de um único modo é equivalente a uma medição óptica heteródina [48]. Teoricamente, ela corresponde a medir um POVM $\Pi(\alpha) = \pi^{-1/2} |\alpha\rangle\langle \alpha|$. Em termos práticos, a medição de ambas as

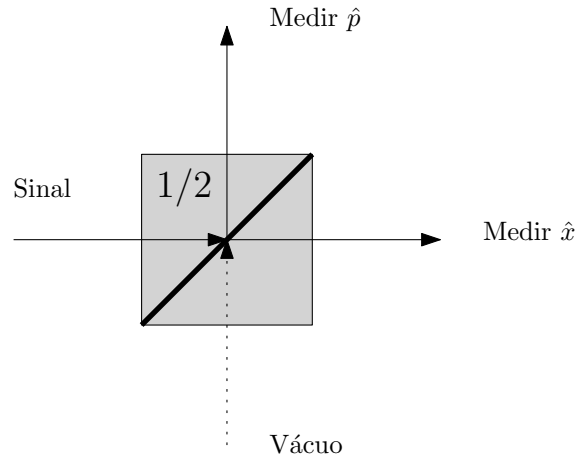


Figura 2.7 Representação da medição simultânea de ambas as quadraturas de um mesmo modo eletromagnético. O sinal é dividido em um BS balanceado. Nos modos de saída são medidas as quadraturas \hat{x} e \hat{p} .

quadraturas pode ser realizada dividindo-se o sinal quântico em um BS balanceado ($\tau = 1/2$), seguido da medição homódina de \hat{x} e \hat{p} nos modos de saída, assim como ilustrado na Figura 2.7. Como o sinal é combinado com um modo de vácuo no BS, o princípio da incerteza de Heisenberg (2.38) não é violado [36].

2.5.1 Medições Homódinas

Na detecção homódina é possível medir as componentes de quadratura do campo [36]. As componentes de quadratura \hat{x}_θ são definidas com relação a uma determinada referência de fase θ , que pode ser variada experimentalmente de acordo com

$$\hat{x}_\theta = \hat{x} \cos \theta + \hat{p} \sin \theta. \quad (2.120)$$

O esquema principal de detecção homódina está ilustrado na Figura 2.8. Nesse esquema, o sinal interfere com um laser coerente em um BS balanceado ($\tau = 1/2$). O laser coerente é chamado de oscilador local e provê a referência de fase θ para a medição da quadratura. Admite-se que o sinal e o oscilador local possuem uma relação de fase fixa, o que é geralmente o caso em virtude de ambos os campos serem geralmente provenientes de um mesmo laser principal. O oscilador local deve ser bastante intenso em relação ao sinal medido a fim de prover uma referência de fase adequada. Dessa forma, ele pode ser tratado classicamente⁴. Após a mistura, cada feixe de saída segue para um fotodetector, normalmente um fotodiodo de resposta linear. As correntes I_1 e I_2 provenientes dos fotodetectores são medidas e subtraídas, gerando a quantidade $I_{21} = I_2 - I_1$, que contém a informação relevante sobre a medição. Isto pode ser verificado, considerando-se

⁴O operador de aniquilação é substituído pela amplitude complexa do modo.

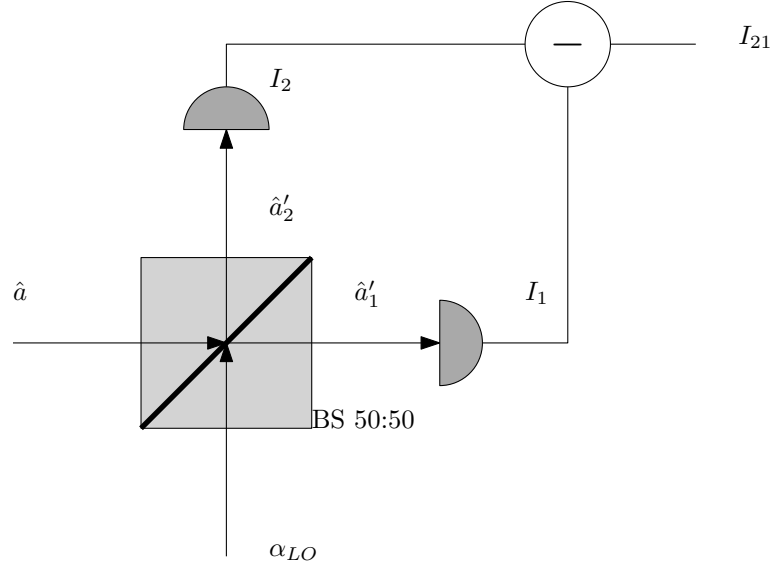


Figura 2.8 Esquema geral de um detector homódino. O sinal a ser medido e o oscilador local são combinados em um divisor de feixe. Os feixes de saída passam por um fotodetector gerando uma corrente elétrica. A quadratura a ser medida é proporcional à diferença das correntes.

que as correntes I_1 e I_2 são proporcionais ao número de fótons \hat{n}_1 e \hat{n}_2 dos feixes que incidem sobre os fotodetectores. Os operadores \hat{n}_1 e \hat{n}_2 podem ser calculados como

$$\hat{n}_1 = \hat{a}'_1{}^\dagger \hat{a}'_1, \quad \hat{n}_2 = \hat{a}'_2{}^\dagger \hat{a}'_2, \quad (2.121)$$

em que

$$\hat{a}'_1 = \frac{1}{\sqrt{2}}(\hat{a} - \alpha_{LO}), \quad \hat{a}'_2 = \frac{1}{\sqrt{2}}(\hat{a} + \alpha_{LO}). \quad (2.122)$$

Neste caso, \hat{a} representa o operador de aniquilação do sinal e α_{LO} , a amplitude complexa do oscilador local. A diferença I_{21} é proporcional à diferença do número de fótons, admitindo-se eficiência quântica perfeita. Usando-se a notação $\hbar = 1$, pode-se mostrar que:

$$\begin{aligned} \hat{n}_{21} &= \hat{n}_2 - \hat{n}_1 = \alpha_{LO}^* \hat{a} + \alpha_{LO} \hat{a}^\dagger \\ &= |\alpha_{LO}| e^{-i\theta} \frac{1}{\sqrt{2}} (\hat{x} + i\hat{p}) + |\alpha_{LO}| e^{i\theta} \frac{1}{\sqrt{2}} (\hat{x} - i\hat{p}) \\ &= \sqrt{2} |\alpha_{LO}| \hat{x}_\theta. \end{aligned} \quad (2.123)$$

Assim, um detector homódino mede a componente de quadratura \hat{x}_θ . A referência de fase é provida pelo oscilador e pode ser variada, permitindo que se possa medir as quadraturas x e p .

2.6 Tópicos de Teoria da Informação

Nas análises de segurança dos protocolos para DQVC são usados conceitos e terminologias da teoria da informação clássica [49] e quântica [45]. Ao longo deste texto, por exemplo, são utilizadas as definições de entropia, informação mútua e capacidade de canal. Essas definições podem ser referentes tanto a variáveis contínuas quanto discretas. Em geral, na passagem do discreto para o contínuo, as somas dão lugar a integrais e as funções probabilidades de massa são substituídas por funções densidade de probabilidade (fdp).

2.6.1 Entropias e Informação Mútua

Considerando-se as variáveis aleatórias discretas X e Y , com distribuição conjunta $p(x, y)$ e marginais $p(x)$ e $p(y)$, respectivamente, a entropia de X , em bits, é dada por:

$$H(X) = - \sum_x p(x) \log_2 p(x). \quad (2.124)$$

A entropia $H(X)$ pode ser interpretada como uma medida da incerteza que se tem sobre a variável X ou ainda como a quantidade de informação que se adquire ao se conhecer os valores de X . De modo análogo, a entropia conjunta de X e Y é definida por:

$$H(X, Y) = - \sum_x \sum_y p(x, y) \log_2 p(x, y). \quad (2.125)$$

Ainda relacionado às distribuições conjuntas, a entropia condicional de Y dado que X é conhecida é definida por:

$$H(Y|X) = \sum_x p(x) H(Y|X = x) = - \sum_x \sum_y p(x, y) \log_2 p(y|x). \quad (2.126)$$

A relação entre as entropias previamente definidas é dada por:

$$H(X, Y) = H(X) + H(Y|X). \quad (2.127)$$

A generalização para um conjunto de variáveis X_1, X_2, \dots, X_n com distribuição conjunta $p(x_1, x_2, \dots, x_n)$ é dada pela regra da cadeia:

$$H(X_1, X_2, \dots, X_n) = \sum_{i=1}^n H(X_i | X_{i-1}, \dots, X_1). \quad (2.128)$$

A informação mútua entre as variáveis X e Y é definida como:

$$I(X; Y) = - \sum_x \sum_y p(x, y) \log_2 \frac{p(x, y)}{p(x)p(y)} dx dy. \quad (2.129)$$

A informação mútua se relaciona com a entropia através das expressões seguintes:

$$I(X; Y) = H(X) - H(X|Y) = H(Y) - H(Y|X) \quad (2.130)$$

$$= H(X) + H(Y) - H(X, Y) = I(Y; X) \quad (2.131)$$

Além disso, $I(X; X) = H(X)$. A informação mútua pode ser interpretada como a redução na incerteza sobre X dado que se conhece Y . Em todas as expressões, o logaritmo foi calculado na base dois (resultado dado em bits). Entretanto, outras bases são possíveis.

Quando X é uma variável aleatória contínua com fdp $f(x)$, a entropia diferencial de X é definida por:

$$h(X) = - \int_S f(x) \log f(x) dx. \quad (2.132)$$

Em que S representa o suporte de X , ou seja, o conjunto de valores de X para os quais $f(x) > 0$. De modo análogo às distribuições discretas, pode-se definir as entropias diferenciais

$$h(X, Y) = - \int \int f(x, y) \log f(x, y) dx dy, \quad (2.133)$$

$$h(X|Y) = - \int \int f(x, y) \log f(x|y) dx dy, \quad (2.134)$$

em que a relação $h(X, Y) = h(X|Y) + h(Y)$ é verificada. A informação mútua entre as variáveis X e Y , com fdp conjunta $f(x, y)$ é definida por:

$$I(X; Y) = - \int \int f(x, y) \log \frac{f(x, y)}{f(x)f(y)}. \quad (2.135)$$

Analogamente ao caso discreto, as seguintes relações são verificadas:

$$I(X; Y) = h(X) - h(X|Y) = h(Y) - h(Y|X) \quad (2.136)$$

$$= h(X) + h(Y) - h(X, Y) = I(Y; X). \quad (2.137)$$

2.6.2 Capacidade de Canal

Um canal discreto é caracterizado como um sistema que consiste em um alfabeto de entrada \mathcal{X} , um alfabeto de saída \mathcal{Y} e uma matriz de transição de probabilidades $p(y|x)$, que expressa a probabilidade de se observar o símbolo y ao se enviar o símbolo x . Para esse canal, a capacidade é definida como

$$C = \max_{p(x)} I(X; Y), \quad (2.138)$$

em que a maximização é realizada sobre todas as distribuições de entrada. Analogamente, pode-se definir a capacidade de um canal contínuo, fazendo a substituição das funções de probabilidade de massa por fdps.

Dentre os diversos modelos de canais existentes, é de grande importância na DQCVC o modelo de canal gaussiano. O canal gaussiano é um canal com alfabeto contínuo, em que a saída Y_i no instante i é a soma da entrada X_i com o ruído gaussiano Z_i , ou seja:

$$Y_i = X_i + Z_i, \quad Z_i \sim \mathcal{N}(0, \sigma_Z^2). \quad (2.139)$$

Admitindo-se que os símbolos de entrada X_i sejam limitados a uma potência P , a capacidade do canal gaussiano pode ser calculada através das entropias diferenciais previamente definidas e é dada por

$$C = \max_{f(x): \langle X^2 \rangle \leq P} I(X; Y) = \frac{1}{2} \log \left(1 + \frac{P}{\sigma_Z^2} \right), \quad (2.140)$$

sendo alcançada quando $X \sim \mathcal{N}(0, P)$. Ou seja, a informação mútua é maximizada quando a distribuição de entrada é gaussiana.

Para o canal gaussiano, a informação mútua pode ser expressada em função da variância condicional de Y dado X , que é definida por:

$$V_{Y|X} = \langle Y^2 \rangle - \frac{\langle XY \rangle^2}{\langle X^2 \rangle} = \langle Z^2 \rangle. \quad (2.141)$$

De modo que,

$$I(X; Y) = \frac{1}{2} \log \left(\frac{\langle Y^2 \rangle}{V_{Y|X}} \right). \quad (2.142)$$

CAPÍTULO 3

Protocolos para DQCVC

Neste capítulo, são descritos e analisados alguns dos principais protocolos existentes para DQCVC. A análise envolve a descrição de todas as etapas dos protocolos, bem como a apresentação de provas de segurança para alguns cenários encontrados na literatura.

3.1 Visão Geral da DQC

Em linhas gerais, um protocolo para DQC do tipo P&M (preparar e medir)¹ consiste das etapas seguintes: geração de variáveis aleatórias por Alice; codificação dessas variáveis em estados quânticos; envio dos estados quânticos a Bob; medição dos estados por Bob; discussão pública entre Alice e Bob através de um canal público autenticado; reconciliação da informação e amplificação de privacidade [5]. Ao final desse processo, se o protocolo de distribuição for bem sucedido, Alice e Bob terão compartilhado bits secretos comuns, que podem ser usados para cifrar mensagens.

Na DQCVC, a informação é codificada nas quadraturas do campo eletromagnético quantizado, que são variáveis contínuas, assim como mostrado no capítulo 2. Nos protocolos considerados, os estados quânticos usados são do tipo gaussiano, tais como os estados coerentes, comprimidos ou o vácuo, destacados na seção 2.3. A informação codificada nas variáveis contínuas pode ser tanto discreta quanto contínua², dependendo do protocolo considerado. Ainda, dependendo do protocolo considerado, a medição das quadraturas pode ser do tipo homódina ou heteródina. No primeiro caso, apenas a quadratura medida é usada para a obtenção da chave, enquanto que, no segundo caso, ambas são utilizadas.

¹Em geral, os protocolos para DQC podem ter uma versão do tipo P&M e uma versão EB (baseada em emaranhamento - *entanglement based*). Normalmente, a versão do tipo P&M é usada nas implementações práticas, enquanto que a versão EB é usada nas provas teóricas de segurança. Em geral, qualquer protocolo do tipo P&M admite uma representação EB [16].

²Nos protocolos encontrados na literatura, a distribuição gaussiana é usada para representar a informação. Por essa razão, normalmente se utiliza o termo *protocolos com modulação gaussiana* para se referir aos protocolos com informação contínua.

Após a medição dos estados recebidos, ocorre uma troca de mensagens através de um canal público autenticado³. Bob pode, por exemplo, informar a Alice sobre quais quadraturas foram medidas, de forma que ela possa manter apenas a informação compatível com estas. Outro tipo de mensagem que precisa ser trocada é referente aos dados de estimação do canal. Normalmente, Alice e Bob divulgam certo percentual de seus dados, de modo que eles possam realizar uma estimativa do canal quântico, e assim, possam avaliar o conhecimento do espião sobre o processo. Após a estimativa da ação do espião, Alice e Bob podem continuar ou abortar o protocolo. Em caso de continuação, ainda são necessárias as etapas de reconciliação da informação e de amplificação de privacidade.

O processo de reconciliação permite que Alice e Bob compartilhem uma sequência binária comum livre de erros. Na DQVC, os protocolos de reconciliação operam em um único sentido, ou seja, os procedimentos de correção de erros são realizados com base em informação adicional enviada de Alice para Bob (reconciliação direta - RD) ou de Bob para Alice (reconciliação reversa - RR). Na RD, Bob deve estimar a sequência de dados de Alice a partir de seus resultados medidos e da informação adicional enviada por Alice. Na RR, Alice é que deve estimar os dados de Bob a partir dos valores por ela gerados e da informação adicional enviada por Bob. Finalmente, os bits reconciliados são transformados em uma chave secreta após a etapa de amplificação de privacidade. Nesse processo, as sequências de dados compartilhadas têm o seu tamanho reduzido, a fim de que Eva tenha informação praticamente nula acerca da chave.

Além da descrição dos protocolos, é necessária a apresentação de provas de segurança que justifiquem que os bits da chave obtidos são seguros. Idealmente, o que se procura é uma prova de segurança incondicional. Nesse tipo de prova, Eva possui recursos ilimitados e pode fazer tudo, exceto violar as leis da mecânica quântica [59]. Em ordem de poder e complexidade crescentes, os ataques de Eva podem ser classificados em individuais, coletivos e coerentes. Em um ataque individual, Eva pode interagir individualmente e da mesma forma com cada estado quântico enviado através do canal. Além disso, a medida de Eva para esse tipo de ataque é realizada antes dos procedimentos clássicos de reconciliação da informação e de amplificação de privacidade ocorrerem. Embora os ataques individuais sejam o tipo de ataque mais limitado, eles ainda são os mais próximos de serem executados com a tecnologia atual. Por outro lado, em um ataque coletivo, Eva continua interagindo individualmente com os estados enviados por Alice, mas ela pode armazenar os seus estados auxiliares em uma memória quântica a fim de realizar uma medida coletiva sobre todos os seus estados após a conclusão do processo de reconciliação. Finalmente, os ataques coerentes são os mais poderosos permitidos pela mecânica quântica. Nesse tipo de ataque, Eva interage globalmente com todos os estados enviados por Alice e realiza uma medição global nos seus estados ao final do processo de reconciliação da informação. Apesar do ataque coerente ser o mais geral, mostra-se em [60] que os ataques coerentes não superam o ataque coletivo ótimo para os protocolos com modulação gaussiana.

³Em um canal público autenticado, Eva pode ler as mensagens que trafegam no canal, livremente, mas não pode alterá-las, nem forjar a identidade de Alice e Bob em mensagens criadas por ela.

Dessa forma, para esses protocolos, o cenário de ataque coletivo do tipo gaussiano é o mais geral.

3.2 Protocolos para DQVC

Nesta seção, alguns dos protocolos principais que foram propostos para DQVC são descritos e analisados. A ordem adotada segue de certa forma a ordem cronológica em que eles foram propostos. É importante ressaltar que antes deles serem propostos, alguns trabalhos de relevância contribuíram com as ideias iniciais para estes protocolos [61–63].

3.2.1 Protocolo com Estados Comprimidos

O protocolo descrito na sequência foi proposto em [64] por Cerf, Lévy e Van Assche. A ideia central é codificar a informação em uma quadratura comprimida, sendo a segurança derivada a partir de relações análogas à de Heisenberg. No capítulo 2, foi visto que os operadores de quadratura \hat{x} e \hat{p} verificam o princípio da incerteza de Heisenberg, resultando na relação (2.38). Em termos das variâncias das quadraturas, a relação de incerteza pode ser representada por $(\Delta\hat{x})^2(\Delta\hat{p})^2 \geq N_0^2$. A igualdade é verificada para estados de incerteza mínima como os estados coerentes, o vácuo e o vácuo comprimido. Como foi mostrado na seção 2.3.4, para esse tipo de estado, quando uma das quadraturas é comprimida, a outra é expandida. Então, $(\Delta\hat{x})^2 < N_0$, se a quadratura \hat{x} for comprimida ou $(\Delta\hat{p})^2 < N_0$, se a quadratura \hat{p} for comprimida. Com isso, o protocolo pode ser descrito nas seguintes etapas:

1. Alice escolhe aleatoriamente a quadratura (base) a ser comprimida de um modo de vácuo. Se ela escolhe a base 1, ela comprime \hat{x} ($(\Delta\hat{x})^2 = \sigma_1^2 < N_0$) e em seguida desloca \hat{x} de um valor x_0 escolhido de acordo com uma distribuição gaussiana de média nula e variância Σ_1^2 (Figura 3.1). Se ela escolhe a base 2, ela comprime \hat{p} ($(\Delta\hat{p})^2 = \sigma_2^2 < N_0$) e em seguida desloca \hat{p} de um valor p_0 escolhido de acordo com uma distribuição gaussiana de média nula e variância Σ_2^2 .
2. Alice envia o estado comprimido para Bob.
3. Alice revela qual foi a base comprimida a Bob, após Bob acusar o recebimento do sinal.
4. Bob realiza a medida na base revelada por Alice.
5. Alice e Bob extraem uma chave secreta a partir dos dados obtidos por Bob e dos valores mantidos por Alice com a aplicação dos procedimentos de reconciliação da informação e de amplificação de privacidade.

O protocolo descrito dessa maneira requer uma memória quântica para armazenar os estados antes que eles sejam medidos. Esse requisito pode ser eliminado fazendo-se com que

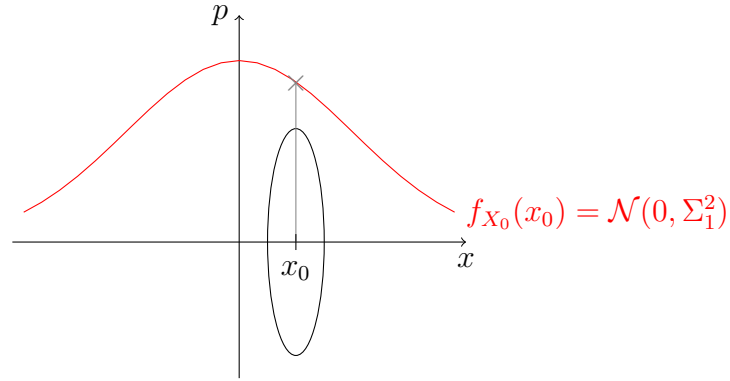


Figura 3.1 A quadratura \hat{x} do vácuo comprimido é deslocada de um valor x_0 escolhido de acordo com uma distribuição gaussiana de média nula e variância Σ_1^2 .

Bob escolha aleatoriamente em que quadratura medir e descartando os dados inconsistentes com as bases usadas por Alice após ela tornar pública essa informação. A informação está codificada na variável x_0 ou p_0 , que possui distribuição gaussiana de média nula e variância Σ_1^2 ou Σ_2^2 , dependendo da base utilizada. Os termos σ_1^2 e σ_2^2 são denominados de variâncias intrínsecas das quadraturas \hat{x} e \hat{p} , respectivamente. Pode-se também definir os parâmetros de compressão das quadraturas como $r_1 \triangleq -\ln(\sigma_1/\sqrt{N_0})$ e $r_2 \triangleq -\ln(\sigma_2/\sqrt{N_0})$. Verifica-se que o parâmetro de compressão é nulo quando não há compressão (estado coerente: $\sigma_1 = \sigma_2 = \sqrt{N_0}$) e positivo quando há compressão na quadratura.

Como restrição de segurança, é requerido que a distribuição dos resultados das medições de \hat{x} seja indistinguível caso Alice tenha usado a base 1 ou 2. Com isso, Eva não obtém nenhuma indicação se ela está medindo um estado comprimido na base 1 ou na base 2. Se a base 1 for usada, as saídas das medidas de \hat{x} possuem uma distribuição gaussiana de variância $\Sigma_1^2 + \sigma_1^2$. Se, ao contrário, a base 2 for usada, as saídas das medidas de \hat{x} possuem uma distribuição gaussiana de variância N_0^2/σ_2^2 , pois $\sigma_1^2\sigma_2^2 = N_0^2$. Assim, requer-se que

$$\Sigma_1^2 + \sigma_1^2 = \frac{N_0^2}{\sigma_2^2}. \quad (3.1)$$

Analogamente, para a quadratura \hat{p} , tem-se que

$$\Sigma_2^2 + \sigma_2^2 = \frac{N_0^2}{\sigma_1^2}. \quad (3.2)$$

Juntando essas duas condições, chega-se à seguinte relação:

$$1 + \frac{\Sigma_1^2}{\sigma_1^2} = 1 + \frac{\Sigma_2^2}{\sigma_2^2} = \frac{N_0^2}{\sigma_1^2\sigma_2^2} = \frac{1}{\alpha^2}. \quad (3.3)$$

Sendo que $\alpha = \sigma_1\sigma_2/N_0 = e^{-(r_1+r_2)}$.

Em um canal gaussiano limitado em potência com SNR γ , a informação mútua máxima que pode ser transmitida através desse canal, em bits por uso, é dada por

$$I_{AB} = \frac{1}{2} \log_2(1 + \gamma), \quad (3.4)$$

sendo $\gamma = \Sigma^2/\sigma^2$ a SNR do canal para uma entrada e ruído de variâncias Σ^2 e σ^2 , respectivamente.

Considerando-se inicialmente a hipótese de ausência de espionagem e transmissão perfeita. Nesse caso, se a base 1 for usada, a SNR é dada por $\gamma_1 = \Sigma_1^2/\sigma_1^2$, enquanto que se a base 2 for usada, a SNR é dada por $\gamma_2 = \Sigma_2^2/\sigma_2^2$. Com a equação (3.3), tem-se que $1 + \gamma_1 = 1 + \gamma_2 = 1/\alpha^2$, de modo que a SNR é igual em ambas as bases. Assim, a informação mútua máxima de Alice para Bob em ambas as bases pode ser expressa como

$$I_{AB} = -\log_2 \alpha = \frac{r_1 + r_2}{\ln 2} \text{ bits por uso.} \quad (3.5)$$

Pode-se observar que para que a informação seja não nula, é necessário que haja compressão nas quadraturas. Como exemplo, considerando o caso em que em ambas as bases se tem 3 dB de compressão ($\sigma^2 = N_0^2/2$ ou $e^r = \sqrt{2}$), tem-se que $\gamma = 3$ e dessa forma $I = 1$ bit de informação para cada estado transmitido.

O modelo usado em [64] é bastante simplificado, pois não foram considerados canais de comunicação com atenuação ou ruído. Além disso, foi considerado apenas um tipo específico de ataque individual em que Eva intercepta os dados de Alice, realiza a medição aleatoriamente nas bases 1 e 2 e reenvia novos estados comprimidos para Bob. Para esse caso, a presença do espião é detectada pelo aumento do ruído e pela consequente diminuição da SNR no lado de Bob. Para avaliar a sua SNR, Bob seleciona um conjunto de valores a fim de compará-los com os valores equivalentes de Alice. Se o canal não foi alvo de interceptação, a diferença entre os dados de Bob e os de Alice deve obedecer a uma distribuição gaussiana com variância σ^2 , considerando que o fator de compressão é o mesmo em ambas as quadraturas. Se o estado de Alice foi interceptado e Eva usou a base correta, a variância dos dados de Bob será $2\sigma^2$. Caso a base usada não seja a correta, a variância será N_0^2/σ^2 . Assim, a variância dos dados de Bob será

$$\frac{1}{2}(2\sigma^2 + \frac{N_0^2}{\sigma^2}) = \sigma^2 + \frac{N_0^2}{2\sigma^2} = \sigma^2 \left[1 + \frac{1}{2\alpha^2} \right]. \quad (3.6)$$

Dessa forma, a SNR calculada por Bob é dada por

$$\frac{\Sigma^2}{\sigma^2 \left[1 + \frac{1}{2\alpha^2} \right]} = \frac{\Sigma^2}{\sigma^2} \left(\frac{2}{3 + \gamma} \right) < \frac{\Sigma^2}{\sigma^2}. \quad (3.7)$$

Nota-se então que a ação de Eva resulta em uma diminuição da SNR no lado de Bob.

Cenários mais realistas para o protocolo com estados comprimidos foram considerados em outros trabalhos. Em [65], foi considerado um canal com atenuação para uma variante desse protocolo. Em [66], foi apresentada uma prova de segurança incondicional. Essa prova explora as conexões existentes entre as técnicas de correção de erros quânticas e a DQC. Apesar de incondicionalmente seguro, o protocolo com estados comprimidos possui uma grande limitação para implementações práticas. Essa limitação está relacionada à perda da compressão nas quadraturas causada pela atenuação do meio. Com isso, a SNR decresce fortemente e o protocolo se torna menos eficiente ou até inseguro [64].

3.2.2 Protocolo com Estados Coerentes

Em 2002, Grosshans e Grangier propuseram em [65] um protocolo para DQCVC que utiliza estados coerentes. Esse protocolo, denominado aqui de GG02, foi demonstrado experimentalmente em [19, 21]. A segurança do protocolo proposto é baseada na versão do teorema da não clonagem para variáveis contínuas [67].

O protocolo GG02 consiste das seguintes etapas:

1. Alice gera dois números aleatórios x_A e p_A a partir de uma distribuição gaussiana com variância $V_A N_0$ (N_0 aqui representa a variância do ruído do vácuo e V_A , um fator de escala).
2. Alice prepara e envia para Bob o estado coerente $|x_A + ip_A\rangle$.
3. Bob escolhe aleatoriamente medir a quadratura \hat{x} ou \hat{p} usando detecção homódina, obtendo os valores x_B ou p_B , respectivamente.
4. Usando um canal público autenticado, Bob informa a Alice qual quadratura foi medida. Dessa forma, metade dos dados gerados por Alice é descartada (referente às quadraturas que não foram medidas por Bob), em média, a fim de manter a consistência dos dados.
5. Ao final da etapa anterior, Alice e Bob terão compartilhado duas sequências de realizações de duas variáveis aleatórias gaussianas correlacionadas. Com isso, eles podem usar um protocolo de reconciliação da informação seguido da amplificação de privacidade a fim de obter uma chave secreta comum.

A segurança do protocolo GG02 foi avaliada em diversos cenários. No artigo pioneiro [65], a análise de segurança ficou restrita a um ataque individual, com um canal caracterizado apenas por um parâmetro de transmissão T e reconciliação no sentido direto. Nesse cenário, o protocolo é considerado seguro para $T > 1/2$, o que limita a utilização do protocolo GG02 a distâncias em torno de 10 km (considerando uma atenuação típica de 0,2 dB/km para uma fibra óptica em 1550 nm). Posteriormente em [19], o cenário de segurança foi expandido, mantendo-se o ataque do tipo individual, mas acrescentando o parâmetro de excesso de ruído ϵ ao canal e

considerando a reconciliação no sentido reverso. Com a mudança no sentido da reconciliação, o protocolo GG02 pode ser considerado seguro para distâncias arbitrárias, desde que ϵ esteja abaixo de um determinado limiar⁴. Por fim, uma prova de segurança para ataques coletivos também foi apresentada. Mostra-se em [68] que o ataque coletivo ótimo é gaussiano. Como mencionado previamente, o cenário de ataque coletivo é o mais geral para um protocolo com modulação gaussiana como o GG02. Na sequência, essas análises de segurança são detalhadas.

Análise de Segurança contra Ataques Individuais e Reconciliação Direta

Quando os ataques considerados são do tipo individual e a reconciliação é do tipo direta, a taxa assintótica de geração de chave em bits por uso do canal é dada por

$$\Delta I = I_{AB} - I_{AE}, \quad (3.8)$$

sendo I_{AB} e I_{AE} a informação mútua entre as variáveis de Alice e Bob e entre Alice e Eva, respectivamente. O termo I_{AB} pode ser calculado da mesma forma que na equação (3.4), bastando para isso utilizar a SNR apropriada. O termo I_{AE} representa a informação adquirida por Eva sobre os estados enviados por Alice. A sua estimativa pressupõe algum tipo de ataque no qual Eva obtém o máximo de informação.

Na estimativa da informação de Eva, considera-se que ambas as quadraturas são atacadas de modo idêntico. Com essa hipótese, pode-se considerar como ataque individual ótimo a aplicação da máquina de clonagem gaussiana descrita em [67]. Com essa operação de clonagem, o ruído adicionado às quadraturas enviadas a Bob e às obtidas por Eva estão relacionados por uma relação de incerteza similar à de Heisenberg. Assim, se a variância do ruído adicionado em uma quadratura de Bob for χN_0 (modelo de ruído equivalente na entrada introduzido na seção 2.4.2), então o mínimo de ruído adicionado na quadratura de Eva possui variância dada por $\chi^{-1} N_0$. O ruído é adicionado em ambas as quadraturas e engloba perdas no meio de transmissão, espionagem ou outras causas. Considerando apenas os efeitos das perdas do meio de transmissão, o meio é caracterizado pelo parâmetro de transmissão T . Dessa forma, $\chi = (1 - T)/T$ assim como mostrado na equação (2.116).

O melhor ataque para Eva consiste em simular o canal, ou seja, capturar uma fração de $1 - T$ do feixe direto do aparato de Alice e enviar através de uma linha sem perdas a fração restante T a Bob [65]. Dessa forma, Eva permaneceria indetectável e obteria a máxima quantidade de informação possível de acordo com o teorema da não clonagem. Sob esse ataque, é possível a obtenção de uma chave secreta desde que $I_{AB} > I_{AE}$, ou seja,

$$\Delta I > 0 \iff \gamma_B > \gamma_E \iff \chi < 1 \iff T > \frac{1}{2}. \quad (3.9)$$

⁴Esse limiar depende dos parâmetros usados.

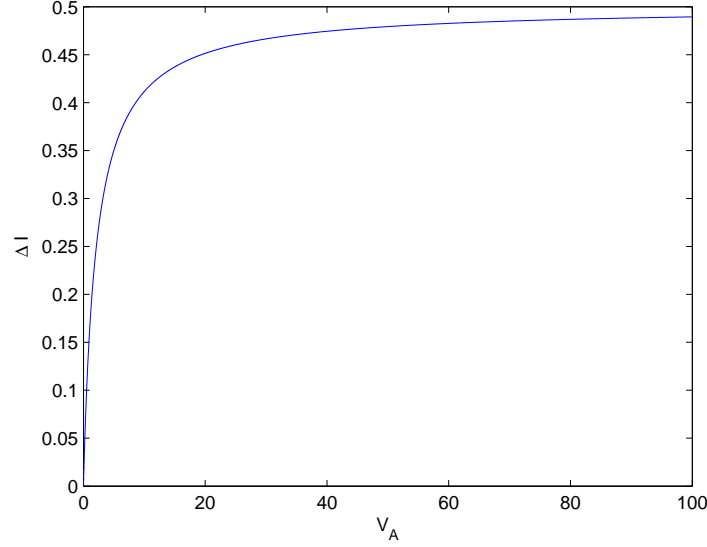


Figura 3.2 Taxa de geração de chave ΔI em função de V_A unidades de N_0 para $\chi = 1/2$ ($T = 2/3$).

Sendo γ_B e γ_E a SNR obtida nas medidas de Bob e Eva, respectivamente. Dessa forma, uma chave secreta pode ser obtida se as perdas na transmissão são menores que 3 dB ($T > 1/2$).

A expressão para a taxa de chave secreta ΔI em função de V_A e T pode ser obtida facilmente a partir das considerações realizadas. Sendo $VN_0 = V_A N_0 + N_0$, a variância de cada quadratura do estado coerente gerado por Alice, pode-se verificar que:

$$1 + \gamma_B = 1 + \frac{V_A N_0}{N_0 + \chi N_0} = \frac{1 + V_A + \chi}{1 + \chi} = \frac{V + \chi}{1 + \chi}, \quad (3.10)$$

$$1 + \gamma_E = 1 + \frac{V_A N_0}{N_0 + \chi^{-1} N_0} = \frac{1 + V_A + \chi^{-1}}{1 + \chi^{-1}} = \frac{V + \chi^{-1}}{1 + \chi^{-1}}. \quad (3.11)$$

Logo,

$$\Delta I = I_{AB} - I_{AE} = \frac{1}{2} \log_2 \left(\frac{1 + \gamma_B}{1 + \gamma_E} \right) = \frac{1}{2} \log_2 \left(\frac{V + \chi}{1 + V\chi} \right). \quad (3.12)$$

Para estados modulados com variância elevada ($\chi V_A \gg 1$ com $\chi < 1$), o valor assintótico de ΔI é dado por

$$\Delta I_{assint} = -\frac{1}{2} \log_2 \chi = \frac{1}{2} \log_2 \frac{T}{1 - T}. \quad (3.13)$$

Na Figura 3.2, é ilustrado o gráfico de ΔI em função de $V_A = V - 1$ para $\chi = 1/2$ ($T = 2/3$ ou 1,76 dB).

Análise de Segurança contra Ataques Individuais e Reconciliação Reversa

Ao mudar o sentido da reconciliação, a taxa de geração de chave para ataques individuais é agora dada por

$$\Delta I_{RR} = I_{AB} - I_{BE}, \quad (3.14)$$

sendo I_{BE} a informação mútua entre as variáveis de Bob e Eva. Nesse cenário com reconciliação reversa, tanto Alice quanto Eva tentam estimar os valores obtidos por Bob nas suas medidas. No que se segue, as variáveis de quadratura de Alice, Bob e Eva são denotadas por $\{x_A, p_A\}$, $\{x_B, p_B\}$ e $\{x_E, p_E\}$, respectivamente. Além dessas, as quadraturas do estado coerente preparado por Alice são denotadas por x_{in} e p_{in} . A partir dessas definições, um modelo de canal pode ser derivado para as quadraturas medidas por Bob de modo similar ao desenvolvido na seção 2.4.2 para modelar a atenuação em um canal. Assim, tem-se que:

$$x_B = \sqrt{T_x}(x_{in} + B_x), \quad (3.15)$$

$$p_B = \sqrt{T_p}(p_{in} + B_p), \quad (3.16)$$

$$\langle x_{in}^2 \rangle = \langle p_{in}^2 \rangle = V N_0 = (V_A + 1)N_0, \quad (3.17)$$

$$\langle x_{in} B_x \rangle = \langle p_{in} B_p \rangle = 0, \quad (3.18)$$

$$\langle B_x^2 \rangle = \chi_x N_0, \quad \langle B_p^2 \rangle = \chi_p N_0. \quad (3.19)$$

Os subscritos x e p levam em conta a possível assimetria dos parâmetros em relação às quadraturas. O parâmetro χ pode ser generalizado de forma a levar em conta a componente de perdas na linha $\chi_{vac} = (1 - T)/T$ mais uma componente adicional ϵ , denominada de excesso de ruído.

Nas análises de segurança, admite-se que Eva controla o canal, ou seja, que através de alguma operação que maximize a sua informação, ela possa forjar o canal entre Alice e Bob descrito pelas equações (3.15-3.19). Nessa operação, Eva procura minimizar as variâncias condicionais $V(x_B|x_E)$ e $V(p_B|p_E)$. Essas variâncias representam a incerteza de Eva sobre as quadraturas de Bob. Assim como na análise do sentido direto, com a aplicação da máquina de clonagem gaussiana, as variâncias condicionais estão sujeitas a uma relação de incerteza dada por

$$V(x_B|x_A)V(p_B|p_E) \geq N_0^2, \quad (3.20)$$

$$V(p_B|p_A)V(x_B|x_E) \geq N_0^2, \quad (3.21)$$

sendo $V(x_B|x_A)$ e $V(p_B|p_A)$ as variâncias das estimativas de Alice sobre as quadraturas de Bob.

A partir das estimativas obtidas por Alice, pode-se mostrar que as variâncias mínimas das estimativas de Eva sobre as quadraturas de Bob são dadas por [19]

$$V(x_B|x_E)_{min} = \frac{N_0}{T_p(\chi_p + V^{-1})}, \quad (3.22)$$

$$V(p_B|p_E)_{min} = \frac{N_0}{T_x(\chi_x + V^{-1})}. \quad (3.23)$$

Além disso, para um estado coerente, as variâncias das estimativas de Alice são dadas por

$$V(x_B|x_A)_{coer} = T_x(\chi_x + 1)N_0, \quad (3.24)$$

$$V(p_B|p_A)_{coer} = T_p(\chi_p + 1)N_0. \quad (3.25)$$

Finalmente, as variâncias calculadas por Bob para suas quadraturas podem ser obtidas a partir das equações (3.15) e (3.16), sendo dadas por

$$V(x_B) = \langle x_B^2 \rangle = T_x(V + \chi_x)N_0, \quad (3.26)$$

$$V(p_B) = \langle p_B^2 \rangle = T_p(V + \chi_p)N_0. \quad (3.27)$$

Admitindo-se que a atenuação e o ruído atuando em ambas as quadraturas sejam idênticos, pode-se calcular as informações mútuas de Alice para Bob e de Bob para Eva como

$$I_{AB} = I_{BA} = \frac{1}{2} \log_2 \frac{V_B}{(V_B|A)_{coer}} = \frac{1}{2} \log_2 \frac{V + \chi}{1 + \chi} = \frac{1}{2} \log_2 \left(1 + \frac{TV_A}{1 + T\epsilon} \right), \quad (3.28)$$

$$I_{BE} = \frac{1}{2} \log_2 \frac{V_B}{(V_B|E)_{min}} = \frac{1}{2} \log_2 [T^2(V + \chi)(V^{-1} + \chi)]. \quad (3.29)$$

Assim, a taxa de geração de chave secreta com reconciliação reversa é dada por

$$\Delta I_{RR} = I_{AB} - I_{BE} = \frac{1}{2} \log_2 \frac{1}{T^2(1 + \chi)(V^{-1} + \chi)}. \quad (3.30)$$

Pode-se verificar que sob perdas altas ($T \ll 1$), o protocolo permanece seguro desde que $\epsilon < (V - 1)/(2V) \approx 1/2$, ou seja, desde que o excesso de ruído esteja abaixo de um determinado limite. Assim, com a reconciliação reversa, pode-se estender o protocolo GG02 para distâncias maiores, superando a limitação dos 3 dB da reconciliação direta, como pode ser observado na Figura 3.3. A limitação final está na eficiência dos protocolos de reconciliação. Eficiências menores que 100% fazem a taxa cair para zero a partir de uma determinada distância.

Análise de Segurança contra Ataques Coletivos e Reconciliação Reversa

Como foi mencionado anteriormente, o cenário de segurança mais geral para o protocolo GG02 envolve ataques coletivos do tipo gaussiano. A prova de segurança para ataques coletivos

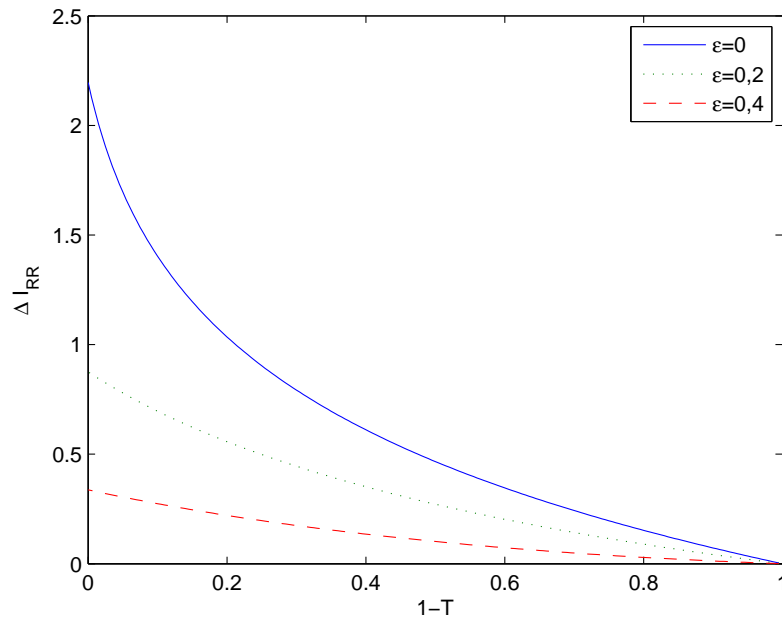


Figura 3.3 Gráfico de ΔI_{RR} versus $1 - T$ para diferentes valores do excesso de ruído e $V_A = 20$ ($V = 21$). Nota-se que com o aumento de ϵ , ΔI_{RR} diminui, mas permanece positiva, desde que $\epsilon < 1/2$.

faz uso da equivalência entre a versão usual dos protocolos do tipo preparar e medir com a versão baseada em emaranhamento (EB - *Entangled Based*) [59], assim como ilustrado na Figura 3.4. Esse tipo de descrição simplifica o cálculo da taxa de geração de chave e proporciona uma descrição unificada de diversos protocolos existentes.

As expressões mostradas a seguir foram obtidas de [21]. Além dos parâmetros considerados na prova de segurança para ataques individuais, foi considerado também nesse artigo a eficiência da detecção homódina do lado de Bob (η) e o ruído eletrônico (v_{el}) na detecção. Dessa forma, o ruído do canal é caracterizado por $\chi_{linha} = 1/T - 1 + \epsilon$, o ruído da detecção homódina por $\chi_{hom} = (1 + v_{el})/\eta - 1$ e o ruído total referente à entrada de Bob por $\chi_{tot} = \chi_{linha} + \chi_{hom}/T$.

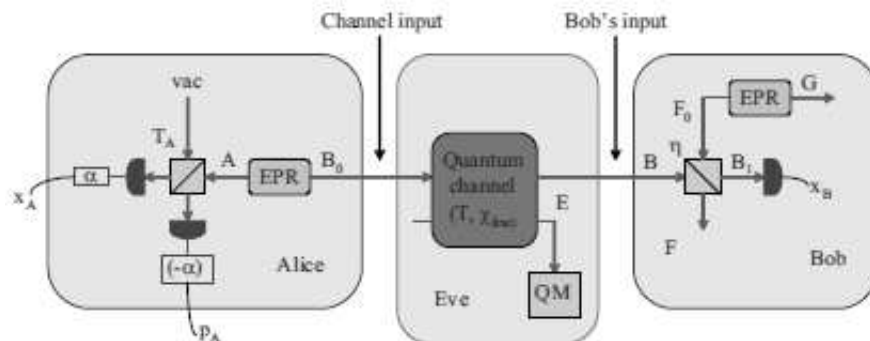


Figura 3.4 Versão EB da DQVC. Alice prepara um estado emaranhado (EPR), envia uma metade a Bob e realiza uma medição na sua parte. Dependendo dos parâmetros usados por Alice, o protocolo pode ser equivalente ao de estados comprimidos ou ao de estados coerentes. Figura obtida de [21].

Quando ataques coletivos são considerados, a informação mútua de Alice para Bob ainda é calculada da mesma forma que para ataques individuais, mas a informação acessível a Eva sobre Bob é dada pela quantidade de Holevo, que para um espectro contínuo é definida como

$$\chi_{BE} = S(\hat{\rho}_E) - \int dx_B p(x_B) S(\hat{\rho}_E^{x_B}), \quad (3.31)$$

sendo $p(x_B)$ a distribuição de probabilidade das medidas de Bob, $\hat{\rho}_E^{x_B}$ o estado do sistema de Eva condicionado à medida x_B de Bob e $S(\hat{\rho})$ a entropia de von Neumann do estado quântico $\hat{\rho}$ [45]. Para um estado gaussiano $\hat{\rho}$ de n modos, $S(\hat{\rho})$ pode ser calculada de acordo com a equação (2.118). A expressão final para χ_{BE} é dada por

$$\chi_{BE} = g(\lambda_1) + g(\lambda_2) - g(\lambda_3) - g(\lambda_4), \quad (3.32)$$

sendo,

$$\lambda_{1,2}^2 = \frac{1}{2}[A \pm \sqrt{A^2 - 4B}], \quad \lambda_{3,4}^2 = \frac{1}{2}[C \pm \sqrt{C^2 - 4D}], \quad (3.33)$$

$$A = V^2(1 - 2T) + 2T + T^2(V + \chi_{linha})^2, \quad B = T^2(V\chi_{linha} + 1)^2, \quad (3.34)$$

$$C = \frac{V\sqrt{B} + T(V + \chi_{linha}) + A\chi_{hom}}{T(V + \chi_{tot})}, \quad D = \sqrt{B}\frac{V + \sqrt{B}\chi_{hom}}{T(V + \chi_{tot})}. \quad (3.35)$$

A taxa de geração de chave é dada por $\Delta I = I_{AB} - \chi_{BE}$, com χ_{BE} calculado de acordo com a equação (3.32) e I_{AB} de acordo com a equação (3.28), substituindo-se χ por χ_{tot} .

3.2.3 Protocolo com Medições Heteródinas

Nos protocolos apresentados nas seções 3.2.1 e 3.2.2, Bob escolhe aleatoriamente se mede a quadratura x ou a quadratura p . Em [30, 69], foi proposta uma variação do protocolo GG02 na qual são medidas ambas as quadraturas de um estado coerente. O protocolo é denominado de NS (*no-switching* - sem comutação) em razão de não ser necessária a escolha aleatória da base de medição. A medição de ambas as quadraturas segue o esquema ilustrado na Figura 2.7. O protocolo NS é descrito pelas seguintes etapas:

1. Alice gera dois números aleatórios x_A e p_A a partir de uma distribuição gaussiana com variância $V_A N_0$.
2. Alice prepara e envia para Bob o estado coerente $|x_A + ip_A\rangle$.
3. Bob mede ambas as quadraturas \hat{x} e \hat{p} usando um esquema de medição como o da Figura 2.7, obtendo os valores x_B e p_B , respectivamente.
4. Ao final da etapa anterior, Alice e Bob terão compartilhado duas sequências de realizações de duas variáveis aleatórias gaussianas correlacionadas. Com isso, eles podem usar um

protocolo de reconciliação da informação seguido da amplificação de privacidade a fim de obter uma chave secreta comum.

Com uma derivação similar à realizada em [19] para ataques individuais com reconciliação reversa, mostra-se em [30] que as taxas de geração de chave do protocolo NS são superiores às do protocolo GG02. Isso se deve ao fato que ambas as quadraturas contribuem para a obtenção da chave secreta. Considerando-se o caso limite em que a variância da modulação de Alice é alta e não há excesso de ruído, as taxas são o dobro das do protocolo GG02 para o tipo de análise considerada. A segurança contra ataques coletivos e reconciliação reversa também pode ser avaliada a partir de uma versão EB do protocolo, assim como mostrado em [59]. A partir dessa análise, verifica-se que, sob limitação do excesso de ruído, o protocolo é seguro para distâncias arbitrárias. Na sequência, a segurança do protocolo NS contra ataques individuais é avaliada. Esse tipo de ataque merece destaque, já que ele foi usado para avaliar a segurança do protocolo proposto nesta tese.

Análise de Segurança contra Ataques Individuais

Na análise de segurança realizada em [30], limitantes para I_{AB} e I_{BE} foram obtidos a partir do cálculo das variâncias, de modo similar ao que foi feito para o protocolo GG02 (equações (3.24-3.27)). Levando em conta o BS de Bob (Figura 3.5), em que o modo antes do BS é denotado por B' , as variâncias referentes à medida de Bob são dadas por:

$$V_{B|A} = \frac{1}{2}(V_{B'|A} + N_0) = \frac{1}{2}[T(\chi + 1) + 1]N_0, \quad (3.36)$$

$$V_B = \frac{1}{2}(V_{B'} + N_0) = \frac{1}{2}[T(V + \chi) + 1]N_0, \quad (3.37)$$

em que $V_{B|A}$ designa $V(x_B|x_A)$ ou $V(p_B|p_A)$, $V_{B'|A}$ é dado pelas equações (3.24) e (3.25) e $V_{B'}$ é dado pelas equações (3.26) e (3.27). Com isso, para o protocolo NS, tem-se que

$$I_{AB} = 2\frac{1}{2}\log_2 \frac{V_B}{V_{B|A}} = \log_2 \left(\frac{T(V + \chi) + 1}{T(\chi + 1) + 1} \right) = \log_2 \left(1 + \frac{TV_A}{2 + T\epsilon} \right), \quad (3.38)$$

sendo que a multiplicação por dois é devido ao fato de ambas as quadraturas contribuírem para a informação total. Nota-se na expressão mais à direita de (3.38) que, devido ao modo do vácuo no BS, a SNR de cada quadratura é diminuída, se comparada ao protocolo GG02 (equação (3.28)). De modo análogo às equações (3.36) e (3.38), uma expressão para $V_{B|E}$ e I_{BE} pode ser obtida a partir das expressões equivalentes para o protocolo GG02. Entretanto, verifica-se que os ataques individuais possíveis não alcançam I_{BE} , sugerindo que o limitante não seja estrito.

Em [70, 71] foram obtidos limitantes para I_{AE} e I_{BE} que são alcançados por ataques ótimos. A abordagem adotada consistiu em caracterizar a transformação simplética S (Figura

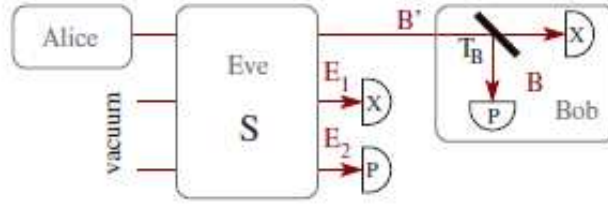


Figura 3.5 Protocolo NS. Bob mede as quadraturas do modo B' . Uma estratégia de espionagem genérica consiste em uma transformação S no modo de Alice e em dois modos auxiliares do vácuo. Figura obtida de [69].

3.5), atuando sobre o modo de Alice e dois modos auxiliares, que maximiza a informação de Eva. De acordo com [71], os limitantes para I_{AE} e I_{BE} são dados por

$$I_{AE} = \log_2 \left(\frac{V + \chi_E}{1 + \chi_E} \right), \quad (3.39)$$

$$I_{BE} = \log_2 \left(\frac{(V + \chi_E)[T(V + \chi) + 1]}{(1 + \chi_E)(V + 1)} \right), \quad (3.40)$$

sendo,

$$\chi_E = \frac{T(2 - \epsilon)^2}{(\sqrt{2 - 2T + T\epsilon} + \sqrt{\epsilon})^2} + 1. \quad (3.41)$$

Ainda em [71], mostra-se que (3.39) e (3.40) são alcançados por quatro tipos diferentes de ataques, dentre os quais o ataque de alimentação direta (*feedforward attack*), que é usado para avaliar a segurança do protocolo proposto nesta tese.

3.2.4 Protocolos com Modulação Discreta

No protocolo GG02, verificou-se que é possível superar a marca dos 3 dB de atenuação do canal passando da reconciliação direta para a reconciliação reversa. Entretanto, devido às imperfeições no processo de reconciliação, as distâncias máximas são na prática limitadas. A introdução de protocolos para DQCVC usando modulações discretas objetiva uma maior eficiência na reconciliação. Dentre esses protocolos, pode-se citar o protocolo de dois estados proposto em [72] e o protocolo de quatro estados em [73].

No protocolo de dois estados, Alice envia a Bob n estados coerentes pertencentes ao conjunto $\mathcal{S}_2 = \{|\alpha e^{-i\pi/4}\rangle, |\alpha e^{i3\pi/4}\rangle\}$, enquanto que no protocolo de quatro estados, os estados são escolhidos no conjunto $\mathcal{S}_4 = \{|\alpha e^{i\pi/4}\rangle, |\alpha e^{i3\pi/4}\rangle, |\alpha e^{i5\pi/4}\rangle, |\alpha e^{i7\pi/4}\rangle\}$. Em ambos os casos α é um número real positivo. Esse esquema de codificação é ilustrado na Figura 3.6.

Para cada estado recebido, Bob realiza uma medição homódina, medindo aleatoriamente a quadratura x ou p . Em ambos os protocolos, Bob obtém uma variável real y_i para $i \in \{1, \dots, n\}$. O sinal de y_i codifica no bit b_i a informação sobre a chave de acordo com a seguinte convenção: $b_i = 1$ se $y_i \geq 0$ e $b_i = 0$ se $y_i < 0$. Como se usa a reconciliação reversa, Alice deve tentar obter a sequência $b = (b_1, \dots, b_n)$ de Bob através de um protocolo de reconci-

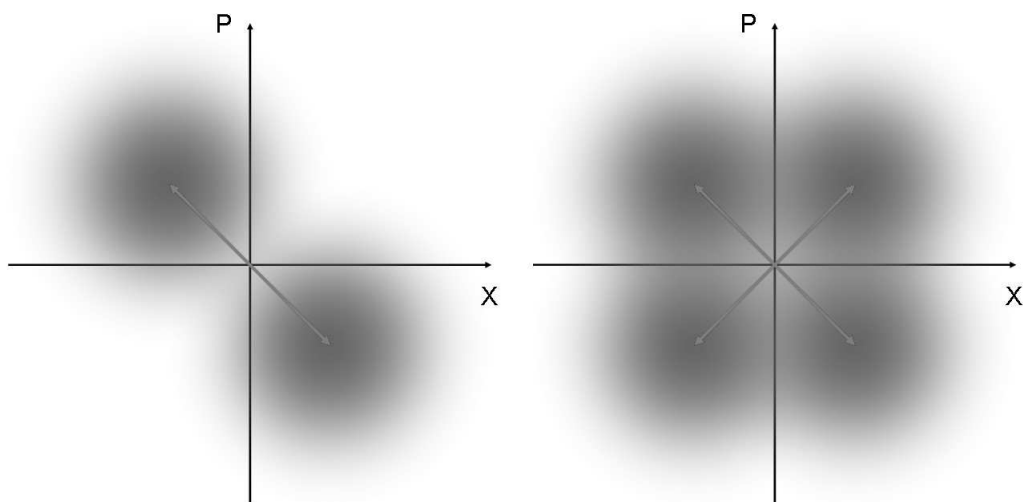


Figura 3.6 Esquema de codificação usado para o protocolo de dois (esquerda) e de quatro estados (direita). Figura obtida de [74].

liação. Para isso, Bob envia a Alice como informação adicional: a quadratura medida (x ou p), o valor absoluto de y_i para $i \in \{1, \dots, n\}$ e a síndrome de b para um código corretor de erros linear com o qual eles concordaram previamente⁵. Com a informação das quadraturas medidas, Alice constrói a sequência $x = (x_1, \dots, x_n)$, em que x_i corresponde ao sinal da quadratura que Bob mediu para o estado que ela enviou, usando a mesma convenção de Bob. Finalmente, com o restante da informação enviada, Alice decodifica a sua sequência a fim de obter a sequência obtida por Bob (seção 3.3.4).

Análise de Segurança

Uma prova contra ataques coletivos para protocolos discretos passa pela construção de uma versão EB do protocolo, assim como foi mostrado anteriormente para o protocolo GG02. Com uma versão EB, Alice e Bob podem calcular χ_{BE} a partir da matriz de covariância de seus estados. Entretanto, para que seja possível construir essa matriz, Alice e Bob precisam estimar os parâmetros T e ϵ a partir dos seus dados. Nos protocolos de dois e de quatro estados, isso foi possível admitindo-se a hipótese de que o canal seja linear [73]. Em um canal linear, a relação entre as quadraturas de Alice e Bob é descrita pelas equações (3.15) e (3.16), sendo o ruído não necessariamente gaussiano. A hipótese de canal linear enfraquece a prova de segurança apresentada em [73], assim como mostrado em [75]. Nesse artigo, foi mostrado que quando Eva usa um amplificador linear sem ruído (NLA - *Noiseless Linear Amplifier*) probabilístico seguido de um ataque de discriminação de estados, a segurança dos protocolos de dois e de quatro estados fica comprometida. O que Eva faz é basicamente amplificar o sinal com sucesso com uma determinada probabilidade e a partir daí, aumentar a chance de discriminar (distinguir)

⁵A síndrome de um código corretor de erros é uma sequência de símbolos (bits) que permite identificar o tipo de erro ocorrido em b , tendo como referência as sequências válidas para o código.

um dos dois (ou quatro) estados corretamente. Em havendo sucesso, ela envia o estado correto para Bob permanecendo indetectável.

A hipótese de canal linear pode ser removida da prova de segurança através da introdução de estados isca (*decoy states*) nos protocolos discretos. A ideia é usar estados com modulação gaussiana para estimar os parâmetros do canal e estados isca para não permitir que o espião possa distinguir entre os estados discretos do protocolo e os usados para estimação [76]. Com isso, os estados usados no protocolo obedecem a relação $p\rho_{chave} + (1 - p)\rho_{isca} = \rho_G$, em que ρ_{chave} é o estado enviado para Bob no protocolo de dois ou de quatro estados, ρ_{isca} é o estado isca e ρ_G é o estado gaussiano usado na estimação de parâmetro. Um ponto ressaltado em [75] é que a preparação de um estado isca é uma tarefa complicada, o que acaba aumentando a dificuldade de se ter implementações práticas de protocolos discretos usando estados isca.

Outra abordagem adotada para a prova de segurança dos protocolos discretos foi adotada em [77]. Essa abordagem não faz uso de estados isca nem de hipóteses de canal linear. A ideia é modificar a versão EB do protocolo de modo que a hipótese de canal linear não seja necessária. Entretanto, modificando a versão EB, modifica-se também a versão prática do tipo preparar e medir e assim, o protocolo não é mais o mesmo descrito no início desta seção.

3.2.5 Outros Protocolos

Como foi discutido na seção 3.2.2, a reconciliação reversa permite que se supere a limitação dos 3 dB na DQCVC. Além disso, a utilização dessa técnica permite que se obtenham expressões fechadas para a taxa de geração de chave secreta como a obtida na equação (3.30) para o protocolo GG02 sob ataques do tipo individual. A outra maneira de superar a limitação dos 3dB e assim aumentar a distância na DQCVC é através da técnica de pós-seleção (*postselection*) [78]. Essa técnica permite que Alice e Bob obtenham uma chave secreta mesmo quando $I_{AB} < I_{AE}$. A ideia central consiste na identificação de regiões em que $I_{AB}(\alpha, \theta, x) > I_{AE}(\alpha, \theta)$, em que α e θ estão relacionadas ao estado transmitido e x representa a variável medida por Bob. Com isso, os resultados das medidas de Bob que caem nessas regiões são usados na obtenção de uma chave, sendo os que ficam fora delas desprezados. Como apenas as regiões que contribuem positivamente para a geração da chave são usadas, é possível estender o protocolo além do limite dos 3 dB com reconciliação direta. A técnica de pós-seleção é usada na análise de segurança de vários protocolos encontrados na literatura como os protocolos discretos com múltiplos símbolos de [79] e [80].

Recentemente, o conceito de protocolos independentes de dispositivo de medição (MDI QKD - *Measurement Device Independent Quantum Key Distribution*) usado na DQC com variáveis discretas foi estendido para a DQCVC [81]. A motivação é projetar um protocolo cuja segurança não seja comprometida por imperfeições nos dispositivos de Alice e Bob. Para isso, existe uma terceira parte não confiável (Charlie) que realiza as medições. Além dos estados

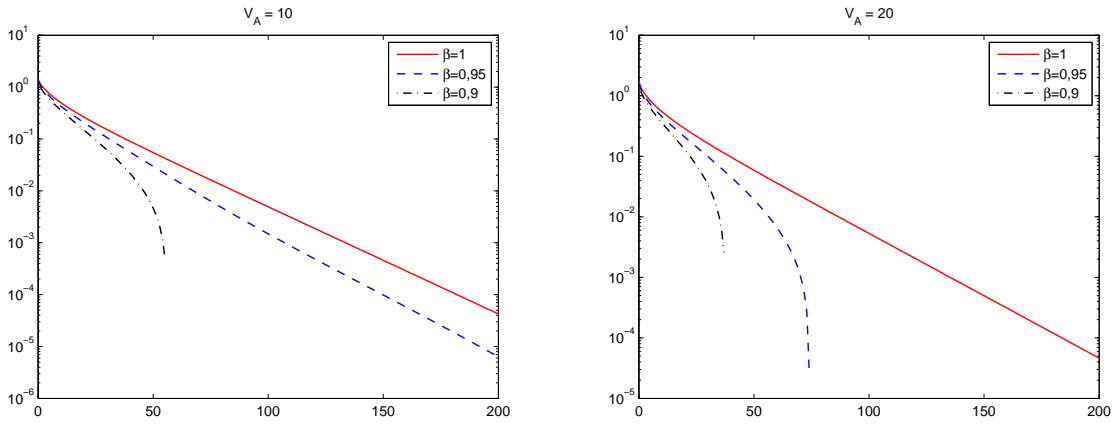


Figura 3.7 Efeito da eficiência de reconciliação nas taxas de geração de chave ΔI em função da distância para o protocolo GG02 sob ataques coletivos. Nesses gráficos, considera-se que a atenuação do canal vale $0,2$ dB/km ($T = 10^{(-0,02d)}$, d em km) e $\epsilon = 0,02$. Na esquerda, $V_A = 10$. Na direita, $V_A = 20$.

coerentes, uma versão de um protocolo independente de dispositivo de medição com estados comprimidos também foi proposta em [82].

3.3 Reconciliação da Informação

Para os protocolos com modulação gaussiana descritos na seção 3.2, foi verificado que desde que o excesso de ruído ϵ esteja abaixo de um determinado limiar, as taxas assintóticas de geração de chave são positivas para distâncias arbitrárias quando a reconciliação reversa é empregada. Além disso, de acordo com a equação (3.28), a informação mútua de Alice para Bob (I_{AB}) poderia ser aumentada indefinidamente aumentando-se a variância $V_A N_0$ da modulação de Alice. Apesar da informação mútua de Bob para Eva (I_{BE}) também crescer com o aumento de V_A , a taxa de geração de chave ainda permaneceria positiva. Entretanto, para isso ocorrer, o processo de reconciliação deveria ser perfeito. Com um processo de reconciliação imperfeito, o termo βI_{AB} ($0 < \beta < 1$) entra no lugar de I_{AB} em ΔI , de modo que quando V_A aumenta, a penalidade imposta pela reconciliação imperfeita $(1 - \beta)I_{AB}$ também aumenta. Dessa forma, um processo de reconciliação imperfeito limita os valores práticos de V_A e assim, quando se somam as perdas e ruído, as distâncias práticas são limitadas pela reconciliação [74]. Com a limitação na variância de Alice, a SNR é basicamente controlada pela distância entre Alice e Bob (TV_A é o termo dominante na SNR - equação (3.28)). O efeito da escolha de V_A e da eficiência de reconciliação β é ilustrado na Figura 3.7.

Sejam X e Y as variáveis aleatórias de Alice e Bob, representando os dados mantidos por eles antes do processo de reconciliação, respectivamente, com $I_{AB} \equiv I(X; Y)$. Com o mesmo protocolo sendo executado nos instantes de tempo $1, \dots, l$, as realizações das variáveis em poder de Alice e Bob são denotadas por X_1, \dots, X_l e Y_1, \dots, Y_l , respectivamente. Admita-se ainda que as variáveis de Alice ou de Bob são independentes de um intervalo de tempo

para outro. Na reconciliação direta, a chave compartilhada é obtida a partir das realizações da variável de Alice, enquanto que na reconciliação reversa a chave é obtida a partir das realizações da variável de Bob. Tomando como exemplo a reconciliação direta⁶, Bob pode obter uma cadeia binária $\Psi(X_{1,\dots,l})$ calculada por Alice a partir de M mensagens trocadas através de um canal público autenticado e de suas realizações Y_1, \dots, Y_l . Comprimindo $\Psi(X_{1,\dots,l})$, Alice e Bob podem obter $lH(\Psi(X))$ bits de informação comuns⁷. Levando em conta que $|M|$ bits⁸ são trocados através do canal público, o processo de reconciliação pode ser projetado para maximizar

$$I_{REC} \triangleq H(\Psi(X)) - \frac{|M|}{l}. \quad (3.42)$$

A partir dessa equação, pode-se definir a eficiência de reconciliação β como

$$\beta \triangleq \frac{I_{REC}}{I(X;Y)}, \quad (3.43)$$

sendo $\beta = 1$ se $I_{REC} = I(X;Y) = I_{AB}$.

A reconciliação da informação pode ser caracterizada como um problema de codificação de fonte com informação paralela (*source coding with side information*). Então, para que Bob obtenha $\Psi(X_{1,\dots,l})$ a partir de Y , é necessário que Alice envie no mínimo $H(\Psi(X)|Y)$ bits por símbolo para Bob [83]. Dessa forma, tem-se que

$$H(\Psi(X)) - \frac{|M|}{l} \leq H(\Psi(X)) - H(\Psi(X)|Y) = I(\Psi(X);Y) \leq I(X;Y), \quad (3.44)$$

em que a última desigualdade⁹ se deve ao fato de que $X \rightarrow \Psi(X) \rightarrow Y$ ($X, \Psi(X)$ e Y formam uma cadeia de Markov) [49]. A partir da relação (3.44), pode-se verificar que uma eficiência próxima de 100% ($\beta = 1$) na reconciliação de variáveis contínuas seria alcançada com uma quantização fina da variável X e com uma troca de mensagens com o mínimo de bits necessário.

Na sequência, são detalhados dois tipos de protocolo para reconciliação de variáveis contínuas gaussianas: o protocolo SEC (*sliced error correction* - correção de erros fatiada) e os protocolos como modulação codificada. Esses protocolos podem ser usados para outras distribuições de probabilidade além da gaussiana, mas o interesse para a DQVCV está restrito ao caso gaussiano.

⁶A passagem para o cenário de reconciliação reversa é trivial, bastando para isso intercambiar as variáveis de Alice e Bob.

⁷ $H(\Psi(X))$ representa a entropia de $\Psi(X)$ em bits por símbolo. Como l símbolos são processados, $lH(\Psi(X))$ bits são obtidos.

⁸O símbolo $|M|$ denota, em geral, a cardinalidade (número de elementos) de um conjunto M . Aqui, ele significa a quantidade de bits que foram trocadas através das M mensagens.

⁹Aplicação de derivações da desigualdade do processamento de dados.

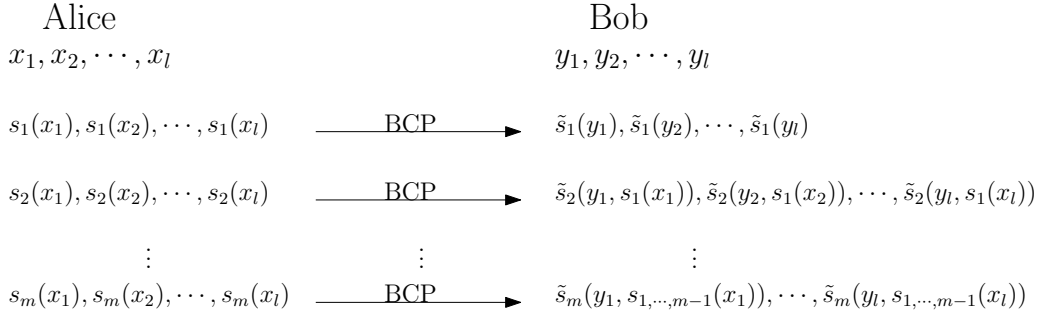


Figura 3.8 Ilustração das etapas do protocolo SEC. A cada etapa um BCP é utilizado de modo a reconciliar as sequências binárias geradas por Alice e Bob.

3.3.1 Protocolo SEC

O protocolo SEC foi proposto em [18] e permite que Alice e Bob possam obter uma sequência binária comum e livre de erros a partir de elementos não binários usando BCPs (*binary correction protocols* - protocolos de reconciliação binária) como primitivas. Sejam X e Y variáveis d -dimensionais em \mathbb{R}^d . Uma função fatiadora (*slice function*) é definida como uma função $S(x)$ que associa uma variável $X \in \mathbb{R}^d$ de Alice a um bit, ou seja, $S(x) : \mathbb{R}^d \rightarrow \{0, 1\}$. Um vetor de fatias (*slice vector*), denotado por $S_{1,\dots,m}(x) = (S_1(x), \dots, S_m(x))$, corresponde a uma cadeia de m bits, de modo que $\Psi(x) = S_{1,\dots,m}(x)$. Do lado de Bob, as estimativas das fatias (*slice estimators*) são denotadas por $\tilde{S}_1(y), \tilde{S}_2(y, S_1(x)), \dots, \tilde{S}_m(y, S_1(x), \dots, S_{m-1}(x))$. A partir dessas definições, o protocolo SEC é descrito pelas etapas seguintes:

Para $i = 1$ até m :

1. Alice calcula a cadeia de l bits $(S_i(x_1), \dots, S_i(x_l))$;
2. Bob prepara a cadeia de l bits $(\tilde{S}_i(y_1, S_{1,\dots,i-1}(x_1)), \dots, \tilde{S}_i(y_l, S_{1,\dots,i-1}(x_l)))$, em que os termos $S_{1,\dots,i-1}(\cdot)$ são conhecidos por Bob, com alta probabilidade, a partir da aplicação de um BCP nos $i - 1$ passos anteriores;
3. Alice e Bob usam um BCP a fim de reconciliar as sequências dos passos 1 e 2 e, dessa forma, Bob adquire o conhecimento de Alice $(S_i(x_1), \dots, S_i(x_l))$.

Após a execução do protocolo, Alice e Bob terão conseguido partilhar $l \times m$ bits comuns a partir de l realizações de suas variáveis e das m fatias (*slices*). Uma ilustração das etapas do protocolo SEC é mostrada na Figura 3.8. Para que o BCP possa reconciliar as sequências binárias de Alice e Bob em cada etapa, é necessário o fornecimento de informação adicional através do canal público autenticado. Essa informação é contabilizada nas M mensagens trocadas durante a execução do protocolo. As funções fatiadoras e os seus estimadores devem ser projetados de modo que a informação trocada nas M mensagens seja a menor possível. Se não for usado o protocolo SEC, o mínimo de informação trocada pode ser calculado de acordo

com [83]. Quando $l \rightarrow \infty$, essa informação é representada pela entropia de $S_{1,\dots,m}(X)$ condicionada a Y , ou seja:

$$I_0 \triangleq H(S_{1,\dots,m}(X)|Y). \quad (3.45)$$

Quando o protocolo SEC é usado, tendo como base um BCP perfeito, a informação mínima a ser trocada é limitada por:

$$\begin{aligned} I_S &\triangleq \sum_{i=0}^m H(S_i(X)|\tilde{S}_i(Y, S_{1,\dots,i-1}(X))) \\ &\stackrel{(a)}{\geq} \sum_{i=0}^m H(S_i(X)|Y, S_{1,\dots,i-1}(X)) \stackrel{(b)}{=} H(S_{1,\dots,m}(X)|Y) = I_0, \end{aligned} \quad (3.46)$$

em que na desigualdade (a) foi usado o fato de que o processamento realizado pelo estimador não fornece mais informação que os parâmetros usados na estimativa. Na igualdade (b), foi usada a regra da cadeia para a entropia condicional. Por fim, pode-se otimizar o BCP para um canal binário simétrico (BSC - *Binary Symmetric Channel*), com probabilidade de erro em cada fatia dada por $e_i = \Pr[S_i(X) \neq \tilde{S}_i(Y, S_{1,\dots,i-1}(X))]$. Dessa forma, com a aplicação da desigualdade de Fano [49] (página 38), pode-se mostrar que

$$\frac{|M|}{l} \equiv I_e \triangleq \sum_{i=1}^m h(e_i) \geq I_S, \quad (3.47)$$

sendo que $h(e_i)$ representa a entropia binária da distribuição $(e_i, 1 - e_i)$. Quando $d \rightarrow \infty$, I_0 , I_S e I_e tendem ao mesmo limite $dH(\Psi(X^{(1)})|Y^{(1)})$ [18]. Ou seja, se os BCPs usados no protocolo SEC são projetados para canais BSC com distribuições $(e_i, 1 - e_i)$, a informação trocada se aproxima do limite teórico de [83] quando d vai para infinito ($|M|/l \equiv I_e \rightarrow I_S$). Assim, o protocolo SEC é assintoticamente ótimo em termos de informação trocada quando o número de dimensões d vai para infinito.

Idealmente o protocolo SEC alcança a eficiência de reconciliação máxima quando $d \rightarrow \infty$. Entretanto, em [18], foi apresentada uma construção do protocolo apenas para $d = 1$. Para esse caso, X e Y são consideradas variáveis escalares reais. A construção envolve o projeto do quantizador, das funções fatiadoras e dos estimadores das funções fatiadoras. A abordagem adotada no projeto dos estimadores \tilde{S}_i consiste em minimizar cada $e_i = \Pr[S_i(X) \neq \tilde{S}_i(Y, S_{1,\dots,i-1}(X))]$ individualmente, já que $h(e_i)$ é crescente no intervalo $[0, 1/2)$. Dessa forma, I_e , dado pela equação (3.47), é minimizado atuando-se em cada estimador independentemente para cada uma das m fatias. Sendo $f(x, y)$ a fdp conjunta de X e Y , a probabilidade de erro em cada fatia (e_i) pode ser expandida como:

$$e_i = \int dy \sum_{b \in \{0,1\}^{i-1}} \Pr[S_i(X) \neq \tilde{S}_i(y, b) \wedge S_{1,\dots,i-1}(X) = b \wedge Y = y]. \quad (3.48)$$

Cada termo é integrado sobre áreas do plano (x, y) que não se sobrepõem: $(x, y) : S_{1, \dots, i-1}(X) = b$. Assim, a minimização pode ser feita em cada termo independentemente. \tilde{S}_i deve satisfazer:

$$\tilde{S}_i(y, b) = \arg \min_{\tilde{s}} Pr[S_i(X) \neq \tilde{s} \wedge S_{1, \dots, i-1}(X) = b \wedge Y = y] \quad (3.49)$$

$$= \arg \max_{\tilde{s}} Pr[S_i(X) = \tilde{s} | S_{1, \dots, i-1}(X) = b \wedge Y = y]. \quad (3.50)$$

A expressão para a probabilidade de erro em função das funções fatiadoras é dada por:

$$e_i = \int dy \sum_{b \in GF(2)^{i-1}} \min_a Pr[S_i(X) = a \wedge S_{1, \dots, i-1}(X) = b \wedge Y = y]. \quad (3.51)$$

As funções fatiadoras são projetadas para a reconciliação de duas variáveis gaussianas $X \sim \mathcal{N}(0, \Sigma^2)$ e $Y = X + \epsilon$ com $\epsilon \sim \mathcal{N}(0, \sigma^2)$. Dessa forma, $Y \sim \mathcal{N}(0, \Sigma^2 + \sigma^2)$ e a fdp conjunta $f_{X,Y}(x, y)$ é dada por

$$f_{X,Y}(x, y) = \frac{1}{2\pi\Sigma\sigma} e^{-x^2/(2\Sigma^2)} e^{-(x-y)^2/(2\sigma^2)}. \quad (3.52)$$

Inicialmente é necessário particionar o domínio de X para em seguida atribuir rótulos a esses intervalos. Denotando-se o processo de particionamento de X por $Q(X)$, o objetivo é fazê-lo de modo que $I(Q(X); Y)$ seja maximizado. No particionamento $Q(X)$, a linha real é dividida em t intervalos, limitados pelas $t - 1$ variáveis $\tau_1, \dots, \tau_{t-1}$. O intervalo a , com $1 \leq a \leq t$ é então definido pelo conjunto $x : \tau_{a-1} \leq x < \tau_a$, em que $\tau_0 = -\infty$ e $\tau_t = +\infty$. Uma expressão para $I(Q(X); Y)$ em função das variâncias de X e Y e dos intervalos da partição pode ser obtida a partir de

$$I(Q(X); Y) \equiv H(Q(X)) + H(Y) - H(Q(X), Y), \quad (3.53)$$

sendo que as entropias são calculadas como

$$H(Q(X)) = - \sum_a P_a \log_2 P_a, \quad (3.54)$$

$$H(Y) = \frac{1}{2} \log_2 2\pi e(\Sigma^2 + \sigma^2), \quad (3.55)$$

$$H(Q(X), Y) = - \sum_a \int_{-\infty}^{\infty} dy f_a(y) \log_2 f_a(y), \quad (3.56)$$

$$P_a = \frac{1}{2} \left[\text{erf} \left(\frac{\tau_a}{\sqrt{2}\Sigma} \right) - \text{erf} \left(\frac{\tau_{a-1}}{\sqrt{2}\Sigma} \right) \right], \quad (3.57)$$

$$\text{erf}(y) = \frac{2}{\sqrt{\pi}} \int_0^y e^{-u^2} du, \quad (3.58)$$

$$f_a(y) = \int_{\tau_{a-1}}^{\tau_a} dx f_{X,Y}(x, y). \quad (3.59)$$

Uma vez que o número de intervalos t é estabelecido, a maximização da equação (3.53) define os intervalos a para as $m = \log_2 t$ (com t escolhido como uma potência de 2) funções fatiadoras. Por fim, resta resolver o problema da rotulagem, ou seja, a atribuição de bits às funções fatiadoras. Como mencionado em [2], o número de possibilidades de atribuição cresce com m , de modo que para valores como $m = 5$, o custo de investigação dessas possibilidades é proibitivo. Entretanto, devido à característica recursiva do protocolo, é razoável admitir que os erros sejam concentrados nas fatias inferiores, de modo que as fatias seguintes sejam facilmente determinadas. Assim, a atribuição adotada segue a regra seguinte: o bit menos significativo de $a - 1$ é atribuído a $S_1(x)$ quando $x : \tau_{a-1} \leq x < \tau_a$; cada um dos bits subsequentes (até o mais significativo) é atribuído a $S_2(x), \dots, S_m(x)$. Dessa forma, a probabilidade de erro e_i é maior para as primeiras fatias.

Como ilustração da construção do protocolo SEC (exemplo retirado de [18]), considere-se o caso em que $m = 1$. Sendo os parâmetros da distribuição conjunta dados por $\Sigma = 1$ e $\sigma = 1/\sqrt{3}$, a SNR equivale a 3. Logo $I(X; Y) = 1$ bit por símbolo. O particionamento ótimo resulta em $I(Q(X); Y) = 0,4850$ (com $H(Q(X)) = 1$; $H(Y) = 2,2546$ e $H(Q(X), Y) = 2,7696$). Os intervalos de quantização são definidos por $\tau_0 = -\infty$, $\tau_1 = 0$ e $\tau_2 = +\infty$. A função fatiadora é dada por

$$S_1(x) = \begin{cases} 0, & x < 0 \\ 1, & x \geq 0 \end{cases}.$$

O estimador da função fatiadora é obtido resolvendo-se

$$\tilde{S}_1(y) = \arg \max_{\tilde{s}} Pr[S_1(X) = \tilde{s} | Y = y].$$

Ou seja, deve-se comparar para os possíveis valores de y as expressões seguintes:

$$\begin{aligned} Pr[S_1(X) = 0 | Y = y] &= Pr[X < 0 | Y = y] = \int_{-\infty}^0 f_{X,Y}(x, y) dx, \\ Pr[S_1(X) = 1 | Y = y] &= Pr[X \geq 0 | Y = y] = \int_0^{\infty} f_{X,Y}(x, y) dx. \end{aligned}$$

Observando-se a Figura 3.9, pode-se observar que

$$\tilde{S}_1(y) = \begin{cases} 0, & y < 0 \\ 1, & y \geq 0 \end{cases}.$$

A probabilidade de erro para a fatia é dada por $e_1 = 0,167$. Consequentemente, a informação mínima a ser trocada é dada por $|M|/l = I_e = h(e_1) = 0,65$ bit por símbolo. Assim, $I_{REC} = 1 - 0,65 = 0,35$ e a eficiência máxima de reconciliação é igual a $\beta = 35\%$ (equações (3.42) e (3.43)).

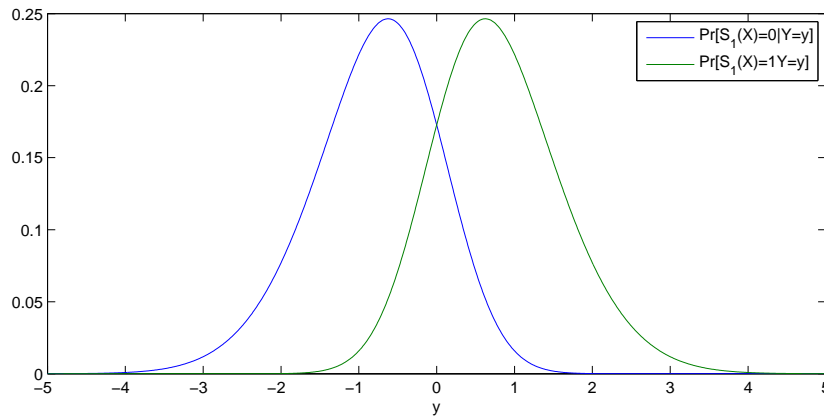


Figura 3.9 Distribuições $\Pr[S_1(X) = 0|Y = y]$ à esquerda e $\Pr[S_1(X) = 1|Y = y]$ à direita

Logicamente, a eficiência da reconciliação pode ser melhorada com o aumento do número de fatias. Em geral, quando se utiliza o protocolo SEC na DQCVC, o número de fatias está entre 4 e 5 [20]. Considerando a mesma SNR do início deste exemplo e $m = 4$ fatias ($t = 16$ intervalos de quantização). O particionamento ótimo resulta em $I(Q(X); Y) = 0,9801$ (com $H(Q(X)) = 3,7836$; $H(Y) = 2,2546$ e $H(Q(X), Y) = 5,0581$), que é bem mais próximo do 1 bit de informação de $I(X; Y)$. A partir do cálculo dos estimadores pode-se verificar que a probabilidade de erro para as fatias são dadas por: $e_1 = 0,4883$, $e_2 = 0,4626$, $e_3 = 0,2508$ e $e_4 = 0,0210$. Verifica-se que as duas primeiras fatias concentram a maior parte dos erros, enquanto que a última possui uma taxa de erros muito baixa. A informação mínima trocada é dada por $|M|/l = I_e = h(e) = h(e_1) + h(e_2) + h(e_3) + h(e_4) = 2,9549$ bit por símbolo. Assim, $I_{REC} = 3,7836 - 2,9549 = 0,83$ e a eficiência máxima de reconciliação é igual a $\beta = 83\%$. Evidentemente essa eficiência máxima pressupõe um BCP que necessite apenas $h(e)$ bits por símbolo na reconciliação, o que não ocorre em situações práticas, assim como discutido posteriormente.

3.3.2 Reconciliação Binária

Os protocolos de reconciliação binária podem operar em um sentido ou em dois sentidos. Como mencionado anteriormente, a reconciliação em um sentido pode ser do tipo direta ou reversa. Por outro lado, a reconciliação em dois sentidos é interativa, ou seja, tanto Alice quanto Bob enviam informações necessárias ao processo de reconciliação. A reconciliação em dois sentidos permite a correção completa dos erros nas sequências divergentes, entretanto a informação trocada pode ser maior que na reconciliação de sentido único, e, dessa forma, a eficiência de reconciliação é reduzida [2].

Um dos primeiros protocolos propostos para reconciliação binária foi o Cascade [84]. Este protocolo é interativo e roda durante um número de passos que é função da probabilidade de erro estimada. Basicamente, a cada passo do protocolo, Alice e Bob enviam uns aos outros

bits de paridade referentes a blocos de dados a fim de que os erros sejam corrigidos. Além do Cascade, existem outros protocolos interativos que podem ser usados, tais como: Furukawa-Yamazaki e Winnow [2]. Para utilizar o Cascade na SEC, é necessário estimar a informação trocada por ele a fim de se obter a eficiência de reconciliação e por consequência, a taxa de geração de chave. Se Alice e Bob possuem cadeias de l bits $A, B \in \text{GF}(2)^l$, respectivamente, então, após rodar o Cascade, eles enviam um ao outro RA (RB) bits, sendo R uma matriz $n \times l$. O valor esperado de n vale aproximadamente $l(1 + \xi)h(e)$, com $e = \Pr[A_j \neq B_j]$ e ξ um pequeno fator de correção. Se $A \rightarrow RA \rightarrow RB$ forma uma cadeia de Markov, Eva não ganha mais informação com RB , de forma que apenas $n \approx l(1 + \xi)h(e)$ são vazados. Em um caso mais geral, se Eva obteve uma informação E espionando o canal quântico, $A|E \rightarrow RA|E \rightarrow RB|E$ não forma necessariamente uma cadeia de Markov. Assim, no pior caso, são liberados $|C| = 2n \approx 2l(1 + \xi)h(e)$ bits de informação na comunicação entre Alice e Bob. Estimativas mais precisas dependem do protocolo usado na DQVC [18].

A reconciliação em um sentido é realizada através do uso de códigos corretores de erros clássicos (CCECs). Em um código de bloco binário \mathcal{C} , com taxa $R = k/n$, k bits de informação são codificados em uma palavra código de n bits, com $n \geq k$. Os $n - k$ bits adicionais introduzidos pelo código fornecem proteção contra erros eventuais que possam ocorrer devido ao ruído introduzido no canal. Os CCECs usados na reconciliação são códigos longos, que operam próximo ao limite de Shannon, como os códigos LDPC. O teorema de Shannon estabelece que para $R < C$ (C , a capacidade do canal), existem códigos de taxa R , com decodificação de máxima verossimilhança, que tem uma probabilidade de erro de decodificação P_E arbitrariamente pequena. Se forem usados códigos de bloco, para $R < C$, existem códigos de comprimento n tal que $P_E \leq 2^{-nE_b(R)}$, em que $E_b(R)$ é uma função positiva de R determinada pelas características do canal [85]. Esse limite para P_E implica que probabilidades de erro arbitrariamente pequenas podem ser alcançadas, usando códigos de bloco com taxa $R < C$, através do aumento de n , mantendo-se constante a razão k/n .

No protocolo SEC, o BCP de cada fatia i é projetado para um canal BSC cujo parâmetro é a probabilidade de erro e_i . Tal modelo de canal possui capacidade dada por $C_i = 1 - h(e_i)$ [49], de modo que os CCECs usados para cada fatia devem possuir taxas R_i próximas de C_i a fim de que a eficiência máxima da SEC seja alcançada.

3.3.3 Modulação Codificada

Em [22, 86, 87], outra abordagem para o problema da reconciliação, inspirada em técnicas de modulação codificada e códigos LDPC, foi proposta. O problema foi caracterizado como um caso de codificação de canal com informação paralela (*channel coding with side information*), que se mostrou equivalente à abordagem usual de codificação de fonte com informação paralela. A reconciliação como um problema de codificação de canal pode ser ilustrada na Figura 3.10. Nela, as variáveis de Alice (X) e Bob (Y) representam a entrada e a saída de um

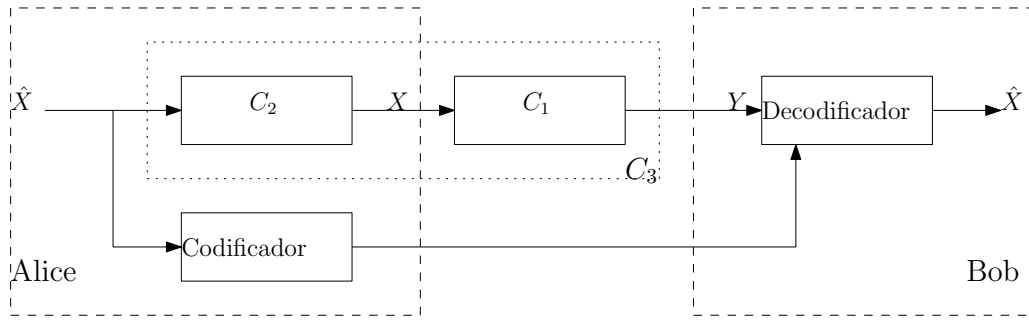


Figura 3.10 Reconciliação como um problema de codificação de canal.

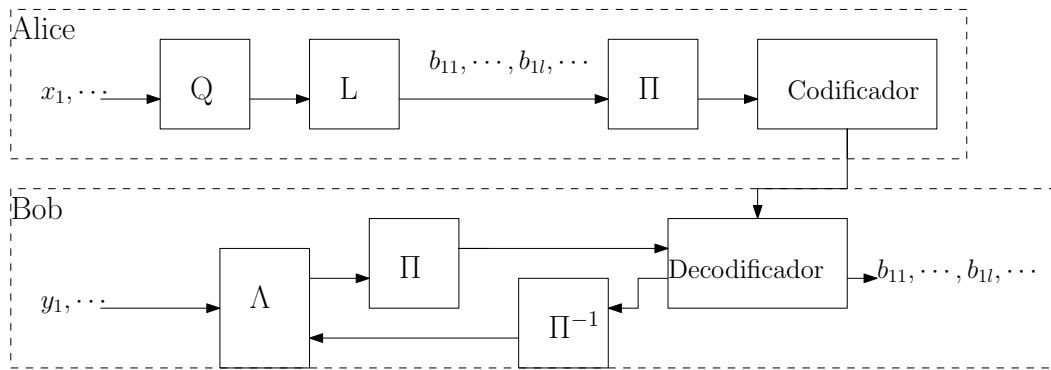


Figura 3.11 Reconciliação com BICM. Os dados de Alice são quantizados (Q), mapeados em bits (L) e entrelaçados (Π). O codificador calcula a síndrome da sequência de símbolos, que é enviada a Bob. Bob decodifica seus dados iterativamente usando a síndrome recebida e uma função dos seus dados (Λ).

canal C_1 , respectivamente. O canal C_2 tem como entrada uma versão quantizada da variável de Alice \hat{X} e como saída a variável X . Se os canais C_1 e C_2 forem concatenados em um canal C_3 , os símbolos contínuos y_i são o resultado da saída do canal C_3 para uma entrada discreta \hat{x}_i . A informação paralela consiste na codificação de \hat{x}_i (a síndrome de um código LDPC) que é enviada através de um canal sem erros e está disponível no decodificador de Bob. A eficiência da reconciliação reside na capacidade de se projetar bons códigos e decodificadores operando em uma taxa próxima a $I(\hat{X}; Y)$ [22].

Nessa abordagem, a etapa de quantização é similar ao protocolo SEC. As variáveis quantizadas \hat{x}_i são discretizadas com l bits e existem funções de rotulação L_m que associam valores de x a um bit para cada nível m , assim como as funções fatiadoras da SEC. O codificador pode usar o mesmo código em todos os níveis como na técnica BICM (*Bit Interleaved Coded Modulation* - Modulação codificada com bits entrelaçados) ou usar um código específico para cada nível como na técnica MLC/MSD (*MultiLevel Coding/MultiStage Decoding* - Codificação multinível/Decodificação multiestágio).

Na reconciliação com BICM, os bits correspondentes aos vários níveis para um conjunto de valores de \hat{x}_i são entrelaçados (permutados) e codificados. A síndrome da sequência binária é passada como informação adicional para Bob para que ele realize a decodificação dos símbolos y_i . Essas etapas são ilustradas na Figura 3.11.

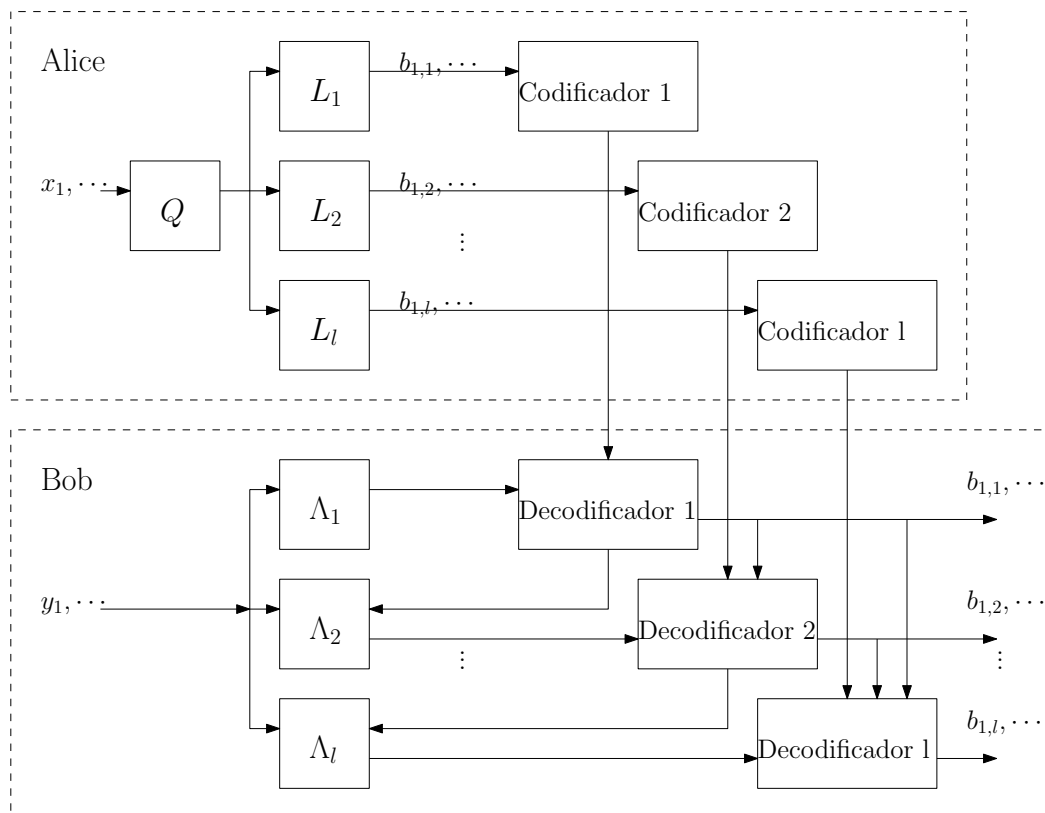


Figura 3.12 Reconciliação com MLC/MSD. Figura adaptada de [22].

Na reconciliação com MLC/MSD, os bits de cada nível (fatias na SEC) são codificados separadamente assim como na SEC. A diferença está no processo de decodificação. Quando se usa MLC/MSD, o decodificador além de produzir os bits de saída decodificados, também gera uma medida de confiabilidade associada a essa decisão (decodificação suave). Essa medida de confiabilidade é usada como informação *a priori* na decodificação de outros níveis, assim como ilustrado na Figura 3.12. A partir dessa descrição, o protocolo SEC é considerado um caso especial da MLC/MSD quando apenas a estimativa dos bits é passada para os estágios seguintes (decodificação abrupta).

A eficiência de reconciliação dos protocolos SEC, BICM e MLC/MSD depende do desempenho da correção binária de erros. Em linhas gerais, nas simulações apresentadas em [22], MLC/MSD é superior a BICM, já que os códigos podem ser otimizados para cada nível. Comparando-se MLC/MSD com SEC, tem-se que o primeiro tem um desempenho superior, mas com uma maior complexidade na decodificação [2, 21]. Entretanto, como tanto MLC/MSD quanto SEC dependem do código utilizado, as eficiências podem ser aumentadas usando-se códigos de comprimento maior e mais eficientes. Em artigo recente, códigos com comprimento da ordem de 2^{20} bits (mais de um milhão) foram usados com SEC e garantiram eficiências superiores a 90% com $m = 5$ fatias [20].

3.3.4 Reconciliação para Modulações Discretas

O processo de reconciliação para os protocolos com modulações discretas, como os apresentados na seção 3.2.4, é mais simples do que para os protocolos com modulações gaussianas. O canal direto é um canal do tipo BI-AWGN¹⁰ com entrada $x = \pm 1$ e saída $y = x + z$ com $z \sim \mathcal{N}(0, \sigma^2)$. O canal reverso também pode ser considerado BI-AWGN, assim como mostrado em [74]. Para isso, Bob calcula os valores u e t a partir de sua variável y da seguinte forma

$$\begin{cases} u &= \frac{y}{|y|} \\ t &= |y|. \end{cases} \quad (3.60)$$

O valor t é enviado como informação adicional para Alice, que por sua vez, calcula a variável v de acordo com

$$v = \begin{cases} t & \text{se } x = 1 \\ -t & \text{se } x = -1. \end{cases} \quad (3.61)$$

Pode-se mostrar que $v = u + w$, com $w = \text{sgn}(xy)z$ ($\text{sgn}(a)$ representa o sinal de a). Dessa forma, $w \sim \mathcal{N}(0, \sigma^2)$ e o canal com entrada u (Bob) e saída v (Alice) pode ser considerado BI-AWGN. A principal motivação na proposição dos protocolos com modulação discreta é a possibilidade de utilizar CCECs já existentes que são otimizados para canais com entrada binária e ruído gaussiano.

3.4 Amplificação de Privacidade

A amplificação de privacidade é um processo que permite que duas partes destilem uma chave secreta a partir de uma variável aleatória comum sobre a qual o espião tem informação parcial. As duas partes não conhecem nada a respeito da informação do espião, exceto que ela satisfaz certa restrição em termos de entropia [88]. Seja W a variável aleatória pertencente a Alice e Bob (n bits resultantes da reconciliação). O espião dispõe de uma variável aleatória V correlacionada com W , que lhe provê no máximo t ($t < n$) bits de informação, ou seja, $H(W|V) \geq n - t$, sendo $H(W|V)$ a entropia condicionada de W dado V ¹¹. O objetivo de Alice e Bob é escolher uma função de compressão $g : \{0, 1\}^n \rightarrow \{0, 1\}^r$, com $r < n$, de tal modo que o conhecimento parcial de Eva sobre W e o conhecimento total sobre g dê a ela arbitrariamente pouca informação sobre $K = g(W)$, exceto com probabilidade desprezível. A variável K resultante é virtualmente uniformemente distribuída¹² dada toda a informação de

¹⁰Um canal BI-AWGN é um canal com entrada binária e ruído AWGN (*Additive White Gaussian Noise* - ruído aditivo gaussiano branco).

¹¹Ela fornece uma medida sobre a incerteza sobre W dado que se conhece V .

¹²Essa condição significa que $H(K|G, V = v) \geq r - \epsilon$ para um ϵ muito pequeno.

Eva e pode assim ser usada como uma chave secreta criptográfica. Uma forma de implementar a amplificação de privacidade é através do uso de funções misturadoras universais (*universal hash functions*) [89]. Com a utilização dessa classe de funções, mostra-se em [88] que $H(K|G, V = v) \geq r - 2^{-s}/\ln 2$ desde que $R(W|V = v) \geq n - t$, sendo $r = n - t - s$ e $R(\cdot)$ a entropia de Rényi de segunda ordem, também conhecida como entropia de colisão. Ou seja, a incerteza de Eva sobre a chave destilada pode se tornar próxima de r ao custo de uma chave menor (s maior, desde que $s < n - t$). Como uma ilustração desse processo, admitindo-se que Alice e Bob reconciliaram $n = 1000$ bits e que Eva conhece no máximo $t = 800$ bits, então empregando-se uma função de compressão com $r = 190$, obtém-se 190 bits seguros de um total de 1000 bits trocados. Nesse caso, $s = 10$ e $H(K|G, V = v) \geq 190 - 0,001$, com uma taxa de geração de chave secreta de 0,19.

CAPÍTULO 4

Mapas de Shannon-Kotel'nikov

Neste capítulo, são introduzidos os mapas de Shannon-Kotel'nikov. Esta nomenclatura, encontrada em [50], se refere à interpretação geométrica de esquemas de codificação conjunta fonte-canal descritos em livros clássicos de telecomunicações [32]. Com essa interpretação, esquemas de modulação analógica tradicionais como o FM (*frequency modulation*) podem ser visualizados como o resultado do mapeamento de um parâmetro (a mensagem) para um ponto em uma curva no espaço de sinais (os símbolos transmitidos no canal). A grande vantagem dessa abordagem é que o desempenho desses esquemas de modulação pode ser relacionado com parâmetros geométricos das curvas, tais como comprimento, curvatura e distância entre dobras. Na sequência deste capítulo, os mapas SK (Shannon-Kotel'nikov) são descritos com base nos seguintes textos [32, 33]. Além dessa descrição geral, são também detalhados mapeamentos específicos usados nesta tese.

4.1 Interpretação Geométrica

O modelo de sistema considerado é mostrado na Figura 4.1. O objetivo é transmitir símbolos de uma fonte que gera dados de amplitude contínua em intervalos de tempo discretos. O transmissor gera formas de onda $s_m(t)$ para cada símbolo m entregue pela fonte. O canal considerado é do tipo AWGN (*additive white gaussian noise* - ruído aditivo gaussiano branco), de modo que o sinal recebido no receptor é simplesmente a soma do sinal transmitido e do ruído. O receptor, por sua vez, produz uma estimativa do símbolo transmitido a partir do sinal recebido. A analogia geométrica surge quando a forma de onda transmitida é representada como um vetor no espaço de sinais. Quando o parâmetro $m \in \mathbb{R}^M$ varia ao longo de seu domínio, o ponto $s(m)$ percorre uma curva em um espaço \mathbb{R}^N . Se $N > M$, os mapeamentos atuam como uma espécie de código corretor de erros analógico, diminuindo assim a distorção entre m e \hat{m} . Esse é o caso de relevância para este trabalho.

Na descrição que se segue, é considerado o caso em que $M = 1$, ou seja, os símbolos da fonte são escalares. Casos em que $M > 1$ são tratados em [51]. Assim, um parâmetro real

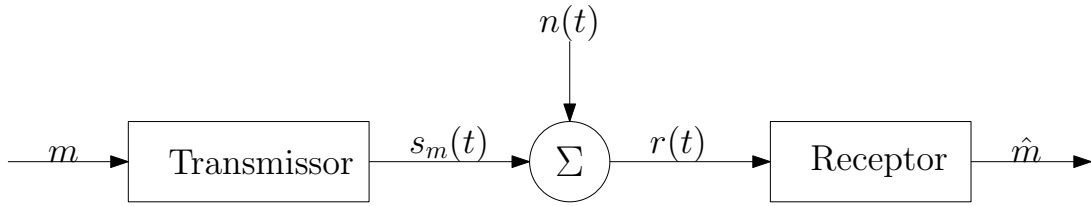


Figura 4.1 Símbolos da fonte m são mapeados pelo transmissor em formas de onda $s_m(t)$. O receptor produz uma estimativa \hat{m} dos símbolos transmitidos com base no sinal ruidoso recebido $r(t)$.

$m \in [-1, 1]$ de uma fonte é mapeado em N coordenadas do canal através de um mapeamento não linear escolhido. A partir da equivalência entre formas de onda e vetores [52], tem-se que para uma determinada base ortonormal $\{\varphi_i\}_{i=1}^N$, as formas de onda do canal podem ser representadas como:

$$\mathbf{s}(m) = [s_1(m) \ s_2(m) \ \cdots \ s_N(m)]. \quad (4.1)$$

Quando m é variado ao longo de seu suporte, a ponta do vetor $\mathbf{s}(m)$ se move ao longo de uma curva, assim como mostrado na Figura 4.2. Assim como o sinal transmitido, o processo de ruído pode ser representado por um vetor \mathbf{n} , de modo que o sinal recebido no receptor é dado por $\mathbf{r} = \mathbf{s}(m) + \mathbf{n}$. Para um canal AWGN com densidade espectral de potência σ_n^2 , um receptor ML (*maximum likelihood* - máxima verossimilhança) produz na sua saída uma estimativa \hat{m} que maximiza a função de verossimilhança dada por:

$$f(\mathbf{r}|m) = f(\mathbf{r} - \mathbf{s}(m)) = \frac{1}{(2\pi\sigma_n^2)^{N/2}} \exp \left\{ -\frac{\|\mathbf{r} - \mathbf{s}(m)\|^2}{2\sigma_n^2} \right\}. \quad (4.2)$$

Esta função é maximizada pelo valor de m que minimiza $\|\mathbf{r} - \mathbf{s}(m)\|$, ou seja, o receptor escolhe o ponto da curva mais próximo do ponto recebido, retornando o \hat{m} referente a esse ponto.

4.1.1 Medidas de Desempenho

Quando os mapas SK são usados para a codificação de sistemas analógicos, é costumeiro se comparar o ganho em SNR da fonte em relação a SNR do canal. Se o canal é AWGN com potência média de entrada P e variância do ruído σ_n^2 , a CSNR (*channel signal-to-noise ratio* - razão sinal-ruído do canal) pode ser definida como $P/(N\sigma_n^2)$. Do lado da fonte, a distorção D entre m e \hat{m} pode ser medida através do MSE (*mean squared error* - erro quadrático médio), de modo que

$$D = \langle (m - \hat{m})^2 \rangle, \quad (4.3)$$

em que foi mantida a notação anterior para a média ou valor esperado. Para uma fonte de informação gaussiana com variância σ_m^2 , pode-se definir a SDR (*source-to-distortion ratio* - razão fonte-distorção) como sendo σ_m^2/D . Assim, o desempenho de um determinado mapa SK pode ser avaliado através de um gráfico da SDR versus CSNR.

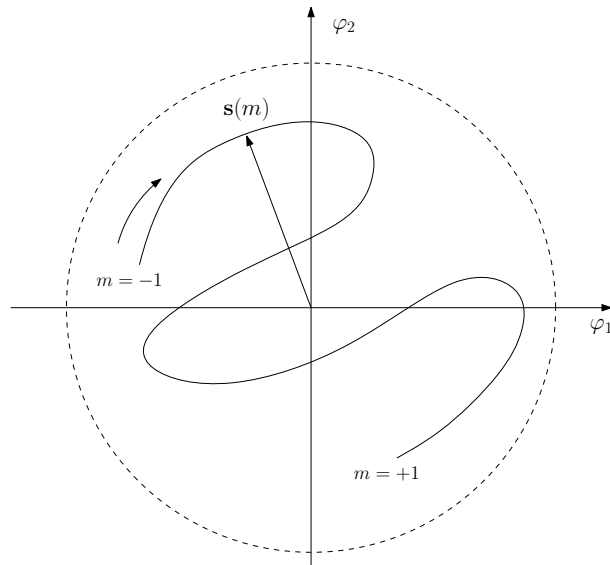


Figura 4.2 Representação genérica de um mapeamento 1:2. Os símbolos da fonte $m \in [-1, 1]$ são mapeados em formas de onda do canal. A ponta do vetor $s(m)$ percorre o *locus* do sinal. O círculo tracejado indica a restrição de potência do canal.

O desempenho de um determinado mapa pode ser comparado com o limitante OPTA (*optimal performance theoretically attainable* - desempenho ótimo teoricamente alcançável). Esse limitante é obtido quando se iguala a função taxa de distorção $R(D)$ à capacidade do canal C [53]. A função taxa de distorção representa a taxa mínima em bits por segundo necessária para descrever uma fonte com distorção D . Por outro lado, a capacidade do canal está ligada ao máximo de informação que pode ser transferida no canal. Para fontes e canais gaussianos, tanto $R(D)$ quanto C possuem expressões bem conhecidas [49]. Admitindo-se que a razão entre a largura de banda do canal e da fonte vale N/M , a igualdade $R(D) = C$ resulta em

$$\frac{\sigma_m^2}{D} = \left(1 + \frac{P}{N\sigma_w^2}\right)^{\frac{N}{M}}. \quad (4.4)$$

O limitante OPTA é ilustrado na Figura 4.3. Pode-se observar que a SDR pode ser melhorada para uma CSNR fixada se a dimensão do canal N é aumentada. Este resultado é conhecido em telecomunicações como um compromisso entre desempenho e largura de banda.

Para mapas práticos, o desempenho em termos da SDR fica distante dos limitantes OPTA, como observado em [50]. Entretanto, em linhas gerais, a tendência de desempenhos melhores para CSNRs mais altas e dimensões mais elevadas é geralmente mantida. Além disso, como mencionado em [54], não existe um único mapa que alcança o melhor desempenho para toda a faixa de CSNRs.

4.1.2 Aproximação de Baixo Ruído

Uma descrição mais detalhada sobre o comportamento dos mapas SK pode ser obtida quando é considerado um regime de baixo nível de ruído. Nesse caso, a distância entre as dobras

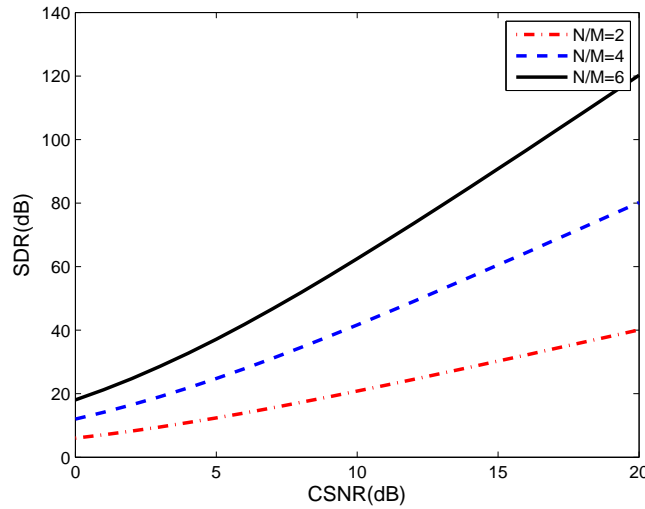


Figura 4.3 Limitante OPTA em função da razão N/M .

da curva, que descreve o mapeamento (Figura 4.2), é maior que três ou quatro vezes o desvio padrão do ruído do canal ($\sqrt{N\sigma_n^2}$).

Admite-se que um símbolo da fonte m_0 corresponde ao ponto da curva $\mathbf{s}(m_0)$. Sob a aproximação de baixo nível de ruído, o ponto recebido \mathbf{r} permanecerá próximo de $\mathbf{s}(m_0)$ com alta probabilidade. Desta forma, a curva pode ser aproximada pela linha reta

$$\mathbf{s}(m) \approx \mathbf{s}(m_0) + (m - m_0)\mathbf{s}'(m_0), \quad (4.5)$$

em que \mathbf{s}' denota a derivada com relação a m . A estimativa do receptor ML pode ser aproximada pela projeção do ponto recebido \mathbf{r} nesta reta. Assim, pode-se mostrar que o MSE condicional é dado por

$$\langle (m - \hat{m})^2 | m = m_0 \rangle = \frac{\sigma_n^2}{\|\mathbf{s}'(m_0)\|^2}. \quad (4.6)$$

Se a fdp de m é denotada por f_m , então a distorção D é obtida calculando-se a média da equação (4.6) sobre o suporte de m , ou seja

$$D = E\{(m - \hat{m})^2\} = \sigma_n^2 \int_{-1}^1 f_m \|\mathbf{s}'(m)\|^{-2} dm. \quad (4.7)$$

É preciso também especificar como os símbolos da fonte m são mapeados no *locus* do sinal. Para um determinado método de modulação, o *locus* corresponde a uma curva de comprimento L (considerando que o suporte de m é finito). Se for introduzida a variável intermediária $l(m)$ denotando o comprimento ao longo da curva, pode-se mostrar que [33]

$$D = \sigma_n^2 \int_{-1}^1 f_m \left| \frac{dl}{dm} \right|^{-2} dm. \quad (4.8)$$

A distorção mínima é alcançada se $l(m)$ é escolhida como

$$l(m) = L \frac{\int_{-1}^m f_u^{1/3} du}{\int_{-1}^1 f_u^{1/3} du} - \frac{L}{2}. \quad (4.9)$$

Esta operação é chamada de *compander* ou uma função de alongamento. Um mapeamento SK pode então ser interpretado como uma combinação de alongamento no suporte seguido da torção da curva. Substituindo-se a equação (4.9) na equação (4.8), tem-se uma expressão para a distorção mínima dada por

$$D_{min} = \frac{\sigma_n^2}{L^2} \left[\int_{-1}^1 f_m^{1/3} dm \right]^3. \quad (4.10)$$

Pode-se observar nessa equação que a distorção (MSE) entre m e \hat{m} pode ser reduzida através do aumento do comprimento da curva. Entretanto, para que isto ocorra, a aproximação de baixo nível de ruído deve ser verificada. Como em geral há uma restrição de potência nos sinais transmitidos pelo canal, aumentar o comprimento da curva tem como efeito reduzir a distância entre as dobras da curva. Dessa forma, a aproximação de baixo ruído pode deixar de ser válida e surge então o efeito de limiar. Nessa situação, a distorção aumenta rapidamente porque os pontos recebidos são decodificados como pontos de dobras diferentes da curva com alta probabilidade.

4.2 Espiral Uniforme de Arquimedes

A espiral uniforme de Arquimedes consiste em duas espirais entrelaçadas em que a distância entre os seus braços é constante, assim como ilustrado na Figura 4.4. Quando usada para mapeamentos SK, uma das espirais é usada para mapear valores negativos do suporte, enquanto a outra é usada para mapear valores positivos. O parâmetro de projeto de uma espiral uniforme de Arquimedes é a distância entre os braços da espiral, aqui denotada por Δ . Na sequência, detalha-se a técnica de projeto para a espiral proposta em [50]. Nessa técnica, uma espiral é projetada para uma determinada CSNR, sendo o canal sujeito a uma restrição de potência média P . Considera-se também que a fonte de informação tem distribuição gaussiana.

Como mencionado anteriormente, um mapeamento SK é composto pelo alongamento do suporte e da torção da curva. Na construção de [50], não foi usada a função de alongamento descrita na equação (4.9). Ao invés dela, foi usada a aproximação do inverso do comprimento da curva dada por $\varphi(x) = \pm \sqrt{|x|/(0,16\Delta)}$. Com essa escolha, os vetores tangente ao longo da curva têm o mesmo comprimento, assim assegurando independência entre o sinal e o ruído. O mapeamento em espiral é descrito por

$$\mathbf{s}(m) = \text{sgn}(m) \frac{\Delta}{\pi} \sqrt{\frac{g_s |m|}{0,16\Delta}} \begin{pmatrix} \cos \sqrt{\frac{g_s |m|}{0,16\Delta}} \\ \text{sen} \sqrt{\frac{g_s |m|}{0,16\Delta}} \end{pmatrix}, \quad (4.11)$$

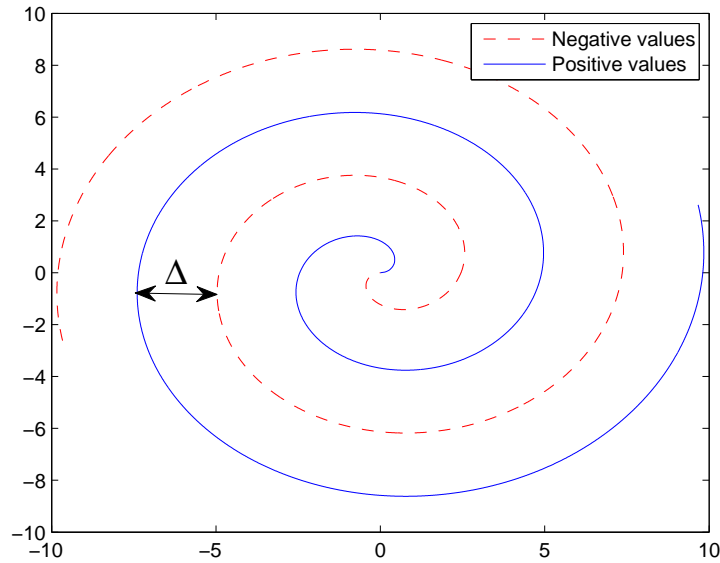


Figura 4.4 Gráfico de uma espiral uniforme de Arquimedes. As linhas tracejadas correspondem ao mapeamento de valores negativos, enquanto as linhas sólidas correspondem ao mapeamento de valores positivos.

em que $\text{sgn}(\cdot)$ denota a função sinal e g_s é um fator de ganho que é necessário para que a restrição de potência seja verificada. A fim de que a curva tenha comprimento finito, o suporte da fonte é truncado no intervalo $m \in [-1, 1]$. Isto significa que os parâmetros de distribuição da fonte tem que ser escolhidos adequadamente a fim de que os efeitos de truncamento possam ser desprezados. Para uma fonte gaussiana de variância σ_m^2 , g_s é dado por

$$g_s = \frac{0,16P\sqrt{2\pi^5}}{\sigma_m\Delta(1 - e^{-1/(2\sigma_m^2)})}. \quad (4.12)$$

Devido à restrição de potência P , um Δ menor resulta em uma espiral com maior comprimento (mais dobras) e como consequência, uma maior SDR, como indicado na equação (4.10). No entanto, se Δ é muito pequeno comparado ao ruído do canal, o efeito de limiar se torna dominante e o desempenho do sistema cai. Assim, existe um compromisso que permite que um valor ótimo para Δ possa ser obtido. Em [50], uma expressão para o Δ ótimo foi obtida a partir da minimização da distorção total (contribuições da distorção com a aproximação de baixo ruído mais a do efeito de limiar). Para $\sigma_m = 0,25$, esta expressão é dada por:

$$\Delta_{opt} = 5,223\sqrt{P}e^{-(3,10^{-4}\text{CSNR}_{dB}^2 + 0,0801\text{CSNR}_{dB})}. \quad (4.13)$$

Deve-se mencionar que o efeito de limiar pode ser bastante severo para o mapeamento em espiral, já que saltos entre dobras adjacentes representam transições de sinal no parâmetro da fonte.

4.3 Geodésicas em Toros Planares

Curvas geodésicas em toros planares foram usadas para a correção de erros em sistemas analógicos em [55]. Estas curvas possuem curvatura constante e giram em torno de um toro planar como uma hélice em um cilindro. Para um toro planar em \mathbb{R}^{2k} , as geodésicas são representadas genericamente por

$$\mathbf{s}_\theta(\alpha) = [r_1 \cos(\omega_1 \alpha), r_1 \sin(\omega_1 \alpha), \dots, r_k \cos(\omega_k \alpha), r_k \sin(\omega_k \alpha)], \quad (4.14)$$

em que $\theta = \{r_1, r_2, \dots, r_k, \omega_1, \omega_2, \dots, \omega_k\}$ é uma parametrização para a curva. Para que a curva seja torcida, é necessário que os elementos ω_i sejam diferentes [56]. O mapeamento com geodésicas pode ser feito aplicando-se a função de alongamento (4.9) aos símbolos da fonte m , para em seguida gerar $N = 2k$ pontos de acordo com (4.14). As propriedades do mapeamento dependem das restrições impostas aos parâmetros θ no seu projeto.

No contexto da DQCVC, é de interesse que se tenha um bom desempenho em baixas CSNRs. Por isso, uma distância maior entre as dobras da curva é mais relevante que o aumento no comprimento da curva. Esses critérios foram levados em conta em [57], de forma que os parâmetros θ foram otimizados a fim de se alcançar bons desempenhos em regiões de baixa CSNR. O processo de otimização consiste em maximizar a função raio circular global (*global circumradius*) sobre θ . O valor mínimo desta função pode ser interpretado como o raio de um tubo centrado ao longo da curva, que previne que haja interseções entre pontos da curva [58]. Dessa forma, a distância mínima entre as dobras da curva equivale ao dobro do valor mínimo da função raio circular global.

A função raio circular global é obtida a partir da função raio circular, que é dada por

$$\rho(\alpha_1, \alpha_2) = \frac{\|\mathbf{s}(\alpha_1) - \mathbf{s}(\alpha_2)\|}{2|\sin \angle(\mathbf{s}(\alpha_1) - \mathbf{s}(\alpha_2), \mathbf{s}'(\alpha_2))|}, \quad (4.15)$$

em que $\angle(\cdot, \cdot)$ denota o ângulo entre dois vetores. Para uma curva suave, a função raio circular global é dada por

$$\rho_g(\alpha) = \min_{\alpha_2} \rho(\alpha, \alpha_2). \quad (4.16)$$

Assim, a distância mínima entre as dobras da curva é dada por

$$d_{min} = 2 \min_{\alpha} \rho_g(\alpha). \quad (4.17)$$

Valores ótimos para θ foram obtidos em [57] para um determinado k através da maximização da equação (4.17) sujeita às seguintes restrições:

$$\|\mathbf{s}_\theta(\alpha)\| = \sum_{i=1}^k r_i^2 = 1, \quad (4.18)$$

$$\|\mathbf{s}_\theta(\alpha)'\| = \sum_{i=1}^k r_i^2 \omega_i^2 = 1, \quad (4.19)$$

$$\omega_i = i\omega_1, i = 1, \dots, k, \quad (4.20)$$

$$\int_{\alpha=-L/2}^{L/2} \|\mathbf{s}_\theta(\alpha)'\| d\alpha = L. \quad (4.21)$$

A restrição (4.18) deve ser aplicada, pois o toro planar está definido em uma esfera unitária em \mathbb{R}^{2k} . De modo análogo, a restrição (4.19) garante que a norma do vetor tangente seja unitária. A restrição (4.20) simplifica o processo de busca da solução ótima restringindo-se a apenas soluções com frequências harmônicas. A última restrição (4.21) evita que a curva se repita a cada período através da restrição do seu comprimento.

CAPÍTULO 5

Mapas de Shannon-Kotel'nikov na DQVC

Neste capítulo são descritas as contribuições propostas nesta tese. Inicialmente, descreve-se um protocolo para DQVC no qual são usados mapas de Shannon-Kotel'nikov na preparação de estados coerentes. Em seguida, detalha-se o modelo de simulação usado para avaliar os ganhos e a segurança do protocolo. Posteriormente, os resultados obtidos com a espiral uniforme de Arquimedes e as curvas geodésicas no toro planar são dispostos e analisados.

A ideia de usar mapeamentos não lineares foi levantada inicialmente em [34]. Nesse artigo, foi proposto um protocolo para DQVC em que os estados coerentes utilizados eram preparados através de um mapeamento com a espiral uniforme de Arquimedes. O intuito do artigo era explorar o efeito de limiar, traduzido pelo aumento da probabilidade de anomalia. A utilização do mapeamento como forma de tornar a DQVC mais robusta, bem como a avaliação da segurança do protocolo foram deixados como possibilidade de trabalhos futuros. Em [35], o mapeamento com a espiral uniforme de Arquimedes foi dimensionado de acordo com a SNR do canal entre Alice e Bob. Nesse artigo, mostrou-se que a utilização do protocolo aumenta a SNR entre as variáveis que são usadas na extração da chave. Além disso, foi realizada uma análise de segurança para o protocolo considerado. Por fim, em artigo submetido para um periódico (apêndice A), foi realizada uma extensão para mapeamentos com curvas no toro planar. Essa extensão permitiu explorar regiões de SNR mais baixas. Além disso, nesse artigo, também foi analisado o efeito do mapeamento na eficiência de reconciliação.

5.1 O Protocolo

O protocolo proposto consiste em usar mapeamentos não lineares, como os descritos no capítulo 4, para preparar estados quânticos coerentes que são enviados por Alice para Bob na DQVC. Sendo mais específico, os valores de deslocamento x_A e p_A no espaço de fase passam agora a ser escolhidos como pontos de uma curva paramétrica. Há uma correspondência

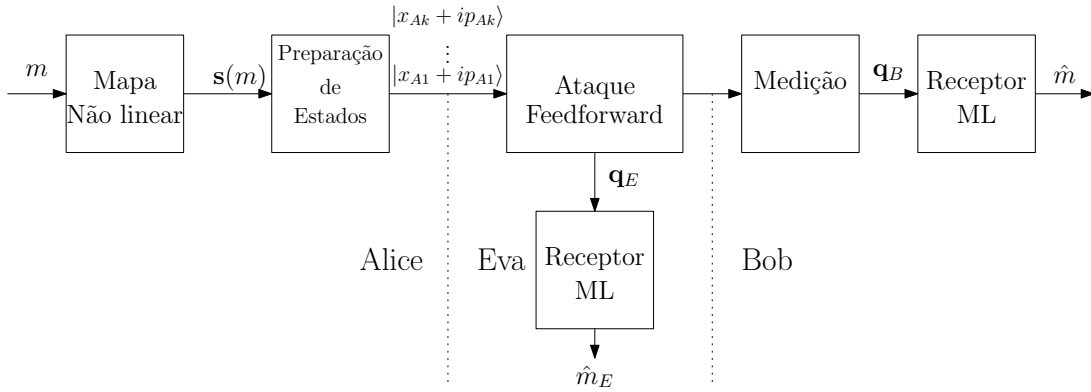


Figura 5.1 Diagrama de blocos do protocolo proposto. Pontos de uma curva são usados para a preparação dos estados coerentes enviados por Alice. Bob e Eva obtêm cada um a sua estimativa do parâmetro escolhido por Alice a partir de seus receptores ML.

unívoca entre pontos nestas curvas e um parâmetro aleatório m , que representa a informação trocada no protocolo. Se os mapas utilizados são ajustados de acordo com o ruído do canal, pode-se melhorar a SNR na comunicação entre Alice e Bob. O diagrama de blocos ilustrando as etapas do protocolo é mostrado na Figura 5.1, sendo essas etapas descritas como:

1. Alice sorteia um número aleatório m a partir de uma distribuição gaussiana $\mathcal{N}(0, \sigma_m^2)$. Então, ela usa esse valor a fim de obter o ponto $\mathbf{s}(m) = [s_1(m) \ s_2(m) \ \cdots \ s_N(m)]$ a partir de um mapeamento em uma curva selecionada em \mathbb{R}^N ($N = 2k$);
2. Alice prepara k estados coerentes $|x_{A(1)} + ip_{A(1)}\rangle, \dots, |x_{A(k)} + ip_{A(k)}\rangle$, em que $x_{A(1)} = s_1(m), p_{A(1)} = s_2(m), \dots, x_{A(k)} = s_{N-1}(m), p_{A(k)} = s_N(m)$, para em seguida enviá-los para Bob;
3. Bob mede ambas as quadraturas x e p dos estados recebidos, para então usar esses resultados e a curva selecionada por eles a fim de obter uma estimativa \hat{m} de m ;
4. Uma chave secreta é extraída a partir de m e \hat{m} após os procedimentos de reconciliação da informação e amplificação de privacidade.

A obtenção da estimativa \hat{m} por Bob pressupõe que ele tenha acesso à versão ruidosa de $\mathbf{s}(m)$, denotada por \mathbf{q}_B . Isso é alcançado no protocolo proposto através da medição de ambas as quadraturas para cada estado coerente enviado. Com isso, o receptor ML de Bob pode projetar o sinal ruidoso na curva e, assim, fornecer uma estimativa \hat{m} do parâmetro escolhido por Alice. Como o protocolo NS é de certa forma subjacente ao protocolo proposto, admite-se que Eva realiza um ataque ótimo para o protocolo NS e utiliza a sua versão ruidosa de $\mathbf{s}(m)$ dada por \mathbf{q}_E para obter a sua própria estimativa \hat{m}_E do parâmetro escolhido por Alice. Para isso, admite-se também que Eva conhece a curva que está sendo usada no mapeamento por Alice e Bob. Dependendo da curva em questão, pode existir algum tipo de ataque mais eficiente para Eva, mas esse fato não foi explorado nesta tese. A análise do desempenho e da segurança do protocolo é feita através de simulações computacionais, cujo modelo é detalhado na sequência.

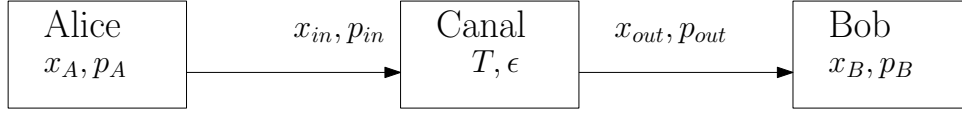


Figura 5.2 Diagrama de blocos para as variáveis de quadratura. As quadraturas de Alice e Bob são denotadas por (x_A, p_A) e (x_B, p_B) , respectivamente. (x_{in}, p_{in}) e (x_{out}, p_{out}) denotam as quadraturas na entrada e na saída do canal, respectivamente.

5.2 Modelo de Simulação

Para simular o protocolo proposto, é necessário descrever como as variáveis de quadratura evoluem ao longo do canal e dispositivos de medição. Em relação à segurança, o protocolo é avaliado para um ataque do tipo alimentação direta (*feedforward*). Esse ataque é um ataque individual ótimo para o protocolo NS descrito na seção 3.2.3 para ambos os tipos de reconciliação de sentido único, ou seja, ele satura os limitantes (3.39) e (3.40) [70, 71]. Para o protocolo proposto, admite-se que Eva realiza esse ataque e usa os resultados das suas medidas para obter a sua própria estimativa usando um receptor ML, assim como indicado na Figura 5.1.

5.2.1 Canal

Conforme mencionado na descrição do protocolo proposto, o protocolo NS é o protocolo subjacente à construção proposta. Na caracterização das quadraturas no protocolo NS, assim como nos demais protocolos descritos na seção 3.2, admite-se que o canal entre Alice e Bob não mistura as quadraturas x e p . Dessa forma, as quadraturas são tratadas como se pertencessem a dois canais independentes. Na Figura 5.2, tem-se uma representação das variáveis de quadratura no canal que liga Alice e Bob. x_A e p_A denotam as variáveis de quadratura escolhidas por Alice, enquanto que x_B e p_B denotam as variáveis medidas por Bob. As quadraturas dos estados coerentes na entrada e na saída do canal são indicadas por x_{in}, p_{in} e x_{out}, p_{out} , respectivamente. O relacionamento entre essas variáveis é dado por

$$x_{in} = x_A + x_{vac}^{(a)}, \quad p_{in} = p_A + p_{vac}^{(a)}, \quad (5.1)$$

$$x_{out} = \sqrt{T}(x_{in} + B_x), \quad p_{out} = \sqrt{T}(p_{in} + B_p), \quad (5.2)$$

$$\langle B_x^2 \rangle = \langle B_p^2 \rangle = \chi N_0 = (1/T - 1 + \epsilon)N_0, \quad (5.3)$$

$$\langle x_{in}^2 \rangle = \langle p_{in}^2 \rangle = V N_0 = (V_A + 1)N_0, \quad (5.4)$$

$$\langle x_{out}^2 \rangle = \langle p_{out}^2 \rangle = (TV_A + 1 + T\epsilon)N_0, \quad (5.5)$$

em que $x_{vac}^{(a)}$ e $p_{vac}^{(a)}$ denotam o ruído do vácuo adicionado às quadraturas x e p na preparação do estado coerente por Alice, respectivamente.

A medição de Bob consiste na divisão do sinal recebido em BS balanceado, seguido da detecção homódina em cada uma das saídas, assim como indicado na seção 2.5. Considerando

um detector homódino ideal e um BS caracterizado pela transformação (2.112) com $\tau = 1/2$, as quadraturas medidas por Bob são dadas por

$$x_B = \frac{1}{\sqrt{2}}(x_{out} + x_{vac}^{(b)}) = \sqrt{\frac{T}{2}}(x_A + x_{vac}^{(a)} + \frac{x_{vac}^{(b)}}{\sqrt{T}} + B_x), \quad (5.6)$$

$$p_B = \frac{1}{\sqrt{2}}(-p_{out} + p_{vac}^{(b)}) = \sqrt{\frac{T}{2}}(-p_A - p_{vac}^{(a)} + \frac{p_{vac}^{(b)}}{\sqrt{T}} + B_p), \quad (5.7)$$

em que $x_{vac}^{(b)}$ e $p_{vac}^{(b)}$ denotam o ruído do vácuo adicionado às quadraturas no BS de Bob. A partir das equações (5.6) e (5.7), pode-se observar que as quadraturas medidas por Bob são compostas por uma componente de sinal (x_A, p_A) mais ruído, de modo que se pode definir uma CSNR para o canal entre Alice e Bob como

$$\text{CSNR}_{AB} = \text{CSNR}_{AB(x)} = \text{CSNR}_{AB(p)} = \frac{TV_A}{2 + T\epsilon}. \quad (5.8)$$

Essa expressão é condizente com a fórmula para I_{AB} dada na equação (3.38).

Os mapas SK introduzidos no capítulo 4 são projetados para canais AWGN. Para converter o canal entre Alice e Bob $(x_A \rightarrow x_B, p_A \rightarrow p_B)$ em um canal AWGN $(x_A \rightarrow x'_B, p_A \rightarrow p'_B)$, pode-se multiplicar as equações (5.6) por $\sqrt{2/T}$ e (5.7) por $-\sqrt{2/T}$ de modo que

$$x'_B = \sqrt{\frac{2}{T}}x_B = x_A + n_x, \quad (5.9)$$

$$p'_B = -\sqrt{\frac{2}{T}}p_B = p_A + n_p, \quad (5.10)$$

em que n_x e n_p são variáveis gaussianas de média nula e variância $(2/T + \epsilon)N_0$.

O ataque implementado por Eva é do tipo *feedforward*, que é um ataque ótimo para o protocolo NS. Esse ataque é ilustrado na Figura 5.3. Como pode ser verificado nessa figura, Eva extrai uma fração $1 - T_E$ do sinal de Alice usando um BS com transmissividade T_E e mede as quadraturas x e p desta fração, obtendo x_E e p_E . Os valores medidos, após a aplicação de um ganho g_E , são usados para ajustar a fração restante T_E do sinal que é enviada para Bob. O canal original, com parâmetros T e ϵ , pode ser forjado por Eva se T_E e g_E são escolhidos como [71]

$$g_E = \sqrt{\epsilon T}, \quad (5.11)$$

$$T_E = \frac{4T(2 - \sqrt{\epsilon(2 - 2T + T\epsilon)})}{(2 + T\epsilon)^2} - \frac{T(2 - \epsilon)}{2 + T\epsilon}. \quad (5.12)$$

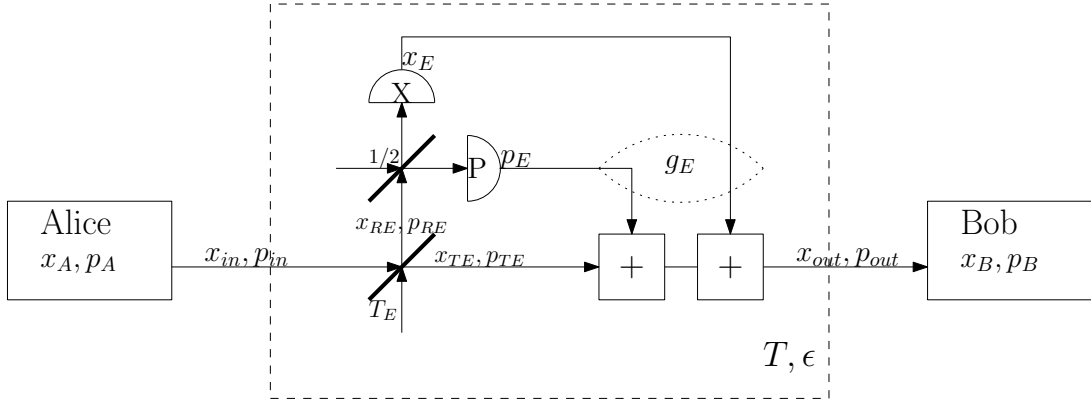


Figura 5.3 Ataque do tipo feedforward. Eva captura uma fração $1 - T_E$ do sinal de entrada. Ela então mede ambas as quadraturas desta fração. Os resultados de sua medição são usados para transladar a fração transmitida T_E do sinal de entrada.

As quadraturas x_E e p_E podem ser caracterizadas de modo similar ao realizado para as quadraturas de Bob. Inicialmente, no primeiro BS, as quadraturas transmitidas e refletidas são representadas respectivamente por

$$x_{TE} = \sqrt{T_E}x_{in} + \sqrt{1 - T_E}x_{vac}^{(e1)}, \quad p_{TE} = \sqrt{T_E}p_{in} + \sqrt{1 - T_E}p_{vac}^{(e1)}, \quad (5.13)$$

$$x_{RE} = -\sqrt{1 - T_E}x_{in} + \sqrt{T_E}x_{vac}^{(e1)}, \quad p_{RE} = -\sqrt{1 - T_E}p_{in} + \sqrt{T_E}p_{vac}^{(e1)}. \quad (5.14)$$

A parte refletida do sinal é medida por Eva, resultando nas quadraturas x_E e p_E dadas por

$$x_E = \frac{1}{\sqrt{2}}(x_{RE} + x_{vac}^{(e2)}) = \sqrt{\frac{1 - T_E}{2}}(-x_A - x_{vac}^{(a)} + \frac{\sqrt{T_E}x_{vac}^{(e1)}}{\sqrt{1 - T_E}} + \frac{x_{vac}^{(e2)}}{\sqrt{1 - T_E}}), \quad (5.15)$$

$$p_E = \frac{1}{\sqrt{2}}(-p_{RE} + p_{vac}^{(e2)}) = \sqrt{\frac{1 - T_E}{2}}(p_A + p_{vac}^{(a)} - \frac{\sqrt{T_E}p_{vac}^{(e1)}}{\sqrt{1 - T_E}} + \frac{p_{vac}^{(e2)}}{\sqrt{1 - T_E}}). \quad (5.16)$$

Analogamente ao canal entre Alice e Bob, a versão AWGN do canal entre Alice e Eva ($x_A \rightarrow x'_E, p_A \rightarrow p'_E$) é obtida multiplicando-se x_E por $-\sqrt{2/(1 - T_E)}$ e p_E por $\sqrt{2/(1 - T_E)}$, resultando em

$$x'_E = -\sqrt{\frac{2}{1 - T_E}}x_E = x_A + n_x^e, \quad (5.17)$$

$$p'_E = \sqrt{\frac{2}{1 - T_E}}p_E = p_A + n_p^e, \quad (5.18)$$

em que n_x^e e n_p^e são variáveis gaussianas de média nula e variância $(2/(1 - T_E))N_0$. A CSNR representando o canal de Alice para Eva é dada por

$$CSNR_{AE} = CSNR_{AE(x)} = CSNR_{AE(p)} = \frac{(1 - T_E)V_A}{2}. \quad (5.19)$$

A parte restante do ataque do tipo *feedforward* consiste na aplicação do ganho g_E a x_E e p_E ,

seguido da translação de x_{TE} e p_{TE} , ou seja

$$x_{out} = -g_E x_E + x_{TE}, \quad (5.20)$$

$$p_{out} = g_E p_E + p_{TE}. \quad (5.21)$$

Se g_E e T_E são escolhido de acordo com as equações (5.11) e (5.12), respectivamente, então as equações (5.20) e (5.21) reproduzem as mesmas estatísticas do canal físico original entre Alice e Bob.

5.2.2 Receptor ML

No protocolo proposto, quando Bob mede as quadraturas dos k estados coerentes enviados por Alice, ele obtém o vetor $\mathbf{q}_B = [x_{B(1)}, p_{B(1)}, \dots, x_{B(k)}, p_{B(k)}]$. Antes de usar o receptor ML, Bob deve ajustar as componentes de \mathbf{q}_B de acordo com as equações (5.9) e (5.10), obtendo \mathbf{q}'_B . Com isso, o receptor ML escolhe \hat{m} como o valor de m para o qual a distância euclidiana entre \mathbf{q}'_B e $s(m)$ é mínima. Da mesma forma, Eva obtém o vetor com as quadraturas medidas denotado por \mathbf{q}_E . Fazendo o ajuste de \mathbf{q}_E de acordo com (5.17) e (5.18), ela obtém \mathbf{q}'_E e assim pode obter a sua própria estimativa \hat{m}_E .

Além do receptor ML, é possível fazer uma decodificação aproximada, dependendo da curva usada. Em [57], é proposto um desses métodos para as curvas geodésicas no toro planar. A vantagem da aproximação é que as operações do receptor são computacionalmente mais simples. Como desvantagem, tem-se uma queda de aproximadamente 2 dB na SDR.

5.2.3 Segurança e Estimação da Informação Mútua

Para avaliar a segurança do protocolo proposto, é necessário calcular as informações mútuas entre as variáveis m , \hat{m} e \hat{m}_E . Define-se então: $I_{AB}^{SK} = I(m; \hat{m})$, $I_{AE}^{SK} = I(m; \hat{m}_E)$ e $I_{BE}^{SK} = I(\hat{m}; \hat{m}_E)$. No cálculo dessas duas últimas, admite-se que Eva implementa o ataque do tipo *feedforward* de modo a maximizar sua quantidade de informação e ao mesmo tempo se manter não detectada. Com o conhecimento da curva usada e a partir das quadraturas medidas, Eva pode obter a sua estimativa \hat{m}_E . Dessa forma, as taxas de geração de chave secreta para o protocolo proposto considerando reconciliação direta e reversa são dadas respectivamente por

$$\Delta I_{DR}^{SK} = I_{AB}^{SK} - I_{AE}^{SK}, \quad (5.22)$$

$$\Delta I_{RR}^{SK} = I_{AB}^{SK} - I_{BE}^{SK}. \quad (5.23)$$

As informações mútuas são estimadas usando o primeiro algoritmo de Kraskov [90]. Esse algoritmo é baseado na estimação da entropia a partir das distâncias dos p vizinhos mais próximos, consistindo em calcular a expressão

$$I^{(1)}(X, Y) = \psi(p) - \langle \psi(n_x + 1) + \psi(n_y + 1) \rangle + \psi(N), \quad (5.24)$$

em que $\psi(x)$ representa a função digama e p , um parâmetro do algoritmo. Ainda nessa expressão, N representa o tamanho das sequências de dados $X = x_1, \dots, x_N$ e $Y = y_1, \dots, y_N$ e $n_x(i)$ ($n_y(i)$) representa o número de pontos x_j (y_j) cuja distância de x_i (y_i) é estritamente menor que $\epsilon(i)/2$, sendo $\epsilon(i)/2$ a distância do ponto $z_i = (x_i, y_i)$ ao p -ésimo vizinho. Com base em uma distribuição gaussiana conhecida, optou-se nas simulações realizadas por $p = 5$ para blocos de $N = 10.000$ amostras. Com essa escolha de parâmetros, pode-se alcançar um erro de estimação da ordem de 10^{-3} , com um tempo razoável de simulação.

5.2.4 Dimensionamento das Curvas

Para a espiral de Arquimedes, cada parâmetro m é mapeado em dois pontos de acordo com a equação (4.11). Esse par de pontos é usado para preparar o estado coerente $|x_{A(1)} + ip_{A(1)}\rangle$ que é enviado para Bob. Para que as curvas tenham comprimento finito, o suporte da fonte de informação é restrito ao intervalo $[-1, 1]$, assim como foi admitido no capítulo 4. Admite-se também que a fonte de informação é gaussiana com média nula e variância $\sigma_m^2 = (0, 25)^2$. A partir dessas escolhas, os efeitos de truncamento podem ser negligenciados. A variância das quadraturas x e p é controlada através do ajuste do ganho g_S (equação 4.12). A potência média do canal P é estabelecida como $V_A N_0$. Com essa escolha, a CSNR por quadratura vale o mesmo que a equação (5.8), de forma que o protocolo pode ser comparado ao protocolo NS.

Uma espiral é projetada para cada valor da transmissão T . Para isso, um Δ_{opt} (equação (4.13)) é calculado para cada T . Nesse cálculo, a CSNR usada é dada por

$$\text{CSNR}_{des} = \frac{P}{\langle n_x^2 \rangle + \langle n_p^2 \rangle} = 0,5 \frac{V_A T}{2 + T\epsilon}. \quad (5.25)$$

Para as simulações com curvas no toro planar, as dimensões simuladas foram $N = \{4, 6\}$. Isso significa que um ponto na curva é usado para preparar dois ou três estados coerentes. Como no caso da espiral, a fonte tem suporte restrito ao intervalo $[-1, 1]$ e é gaussiana com média nula e variância $\sigma_m^2 = (0, 25)^2$. Antes do mapeamento na curva, os símbolos da fonte passam por um *compander* (equação (4.9)). Para efeito de comparação com outros protocolos, os vetores gerados pela curva (4.14) são multiplicados por \sqrt{P} , em que P é a potência média na entrada do canal. Com $P = NV_A N_0$, a CSNR média por quadratura equivale a equação (5.8). Ao contrário do mapeamento em espiral em que mapas são projetados para cada valor de T , uma única curva no toro planar é usada para todos os valores de T na faixa simulada (N

fixo). Uma consequência direta dessa escolha é que o efeito de limiar é mais pronunciado para valores pequenos de T .

5.3 Simulações e Resultados

O protocolo proposto foi simulado para a espiral uniforme de Arquimedes e para as curvas geodésicas no toro planar com $N = 4$ e $N = 6$. O código fonte referente a duas dessas simulações está indicado no apêndice B. Esse código consiste em *scripts* escritos para MATLAB. Além do código próprio desenvolvido, foi usada uma função disponibilizada publicamente para calcular o estimador de Kraskov.

5.3.1 Simulações

Em ambos os tipos de curvas, o parâmetro a ser variado é a transmissão T . São realizadas $NInt$ iterações para produzir um conjunto de resultados. Cada curva é discretizada em $nSIntervals$ intervalos a fim de se realizar a decodificação ML.

O protocolo se inicia com a geração de $NInt$ símbolos da fonte, que são usados para gerar $NInt$ vetores na curva paramétrica. Esses vetores representam os deslocamentos usados para gerar os $NInt$ estados coerentes do protocolo. Em seguida, os estados gerados entram no canal, que consiste na implementação do ataque do tipo *feedforward*. Nas etapas seguintes, há o ajuste das quadraturas de Bob e Eva para que eles realizem a decodificação ML. No caso de Bob, os valores estimados de T são usados para realizar esse ajuste, enquanto que para Eva são usados os valores calculados de T_E . A decodificação ML consiste em se calcular a distância entre o estado medido por Bob ou Eva para cada um dos pontos da curva discretizada, a fim de se escolher a menor distância. Finalmente, os pontos escolhidos na curva são usados para produzir as estimativas dos símbolos da fonte, tanto para Bob quanto para Eva.

As estimativas produzidas são usadas para o cálculo das SNRs, que são usadas para avaliar o ganho do protocolo. Em relação ao cálculo da informação mútua, apenas uma parte das $NInt$ estimativas obtidas é usada na função que calcula o estimador de Kraskov. Isso se deve ao fato de que o tempo de simulação se tornaria proibitivo caso todas as amostras fossem utilizadas. Para usar o estimador de Kraskov, adiciona-se um pequeno ruído aos dados de entrada. Essa operação se faz necessária a fim de evitar que os valores se repitam devido à discretização da fonte.

5.3.2 Resultados

Como foi mencionado no capítulo 4, o ganho de um mapa SK pode ser mostrado através de um gráfico da SDR versus a CSNR. Ambas SDR e CSNR são tipos de SNR, mas a SDR se refere à fonte de informação, enquanto que a CSNR se refere ao canal. A CSNR referente aos protocolos para DQCVC é função do parâmetro de transmissão T , que por sua vez varia entre

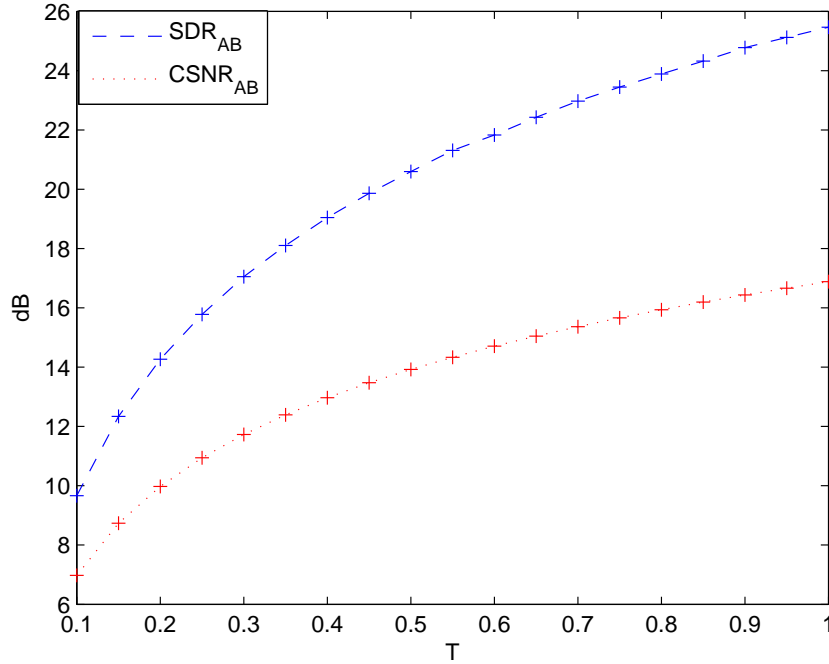


Figura 5.4 Valores simulados para a $SDR_{AB} = \sigma_m^2/D$ comparados com a $CSNR_{AB}$ para o protocolo NS. Observa-se que a diferença entre SDR_{AB} e $CSNR_{AB}$ aumenta para CSNRs mais elevadas (valores maiores de T).

zero e um. Como o protocolo NS é subjacente à construção proposta, optou-se pela comparação da SDR do protocolo proposto com a CSNR do protocolo NS variando-se T . Simulações foram realizadas variando-se os valores de V_A , ϵ além do tipo de curva. A partir das informações mútuas I_{AB}^{SK} , I_{AE}^{SK} e I_{BE}^{SK} para o protocolo proposto, calculam-se as razões $\beta_{lim}^{DR}(SK) \equiv I_{AE}^{SK}/I_{AB}^{SK}$ e $\beta_{lim}^{RR}(SK) \equiv I_{BE}^{SK}/I_{AB}^{SK}$ que representam as eficiências de reconciliação mínimas para a reconciliação direta e reversa, respectivamente. Para comparar com o protocolo NS, define-se também as razões $\beta_{lim}^{DR}(NS) \equiv I_{AE}/I_{AB}$ e $\beta_{lim}^{RR}(NS) \equiv I_{BE}/I_{AB}$ com I_{AB} , I_{AE} e I_{BE} obtidos através dos limitantes dados pelas equações (3.38), (3.39) e (3.40), respectivamente.

Inicialmente, considerou-se o protocolo com a espiral de Arquimedes, sendo $V_A = 100$, $\epsilon = 0,05$ e valores de $T \in [0, 1; 1]$. Os gráficos obtidos para a SDR e a CSNR (equação (5.8)) são mostrados na Figura 5.4. Observa-se que o ganho do protocolo proposto (diferença entre a SDR e a CSNR) diminui com T . As informações mútuas I_{AB}^{SK} , I_{AE}^{SK} e I_{BE}^{SK} são mostradas na Figura 5.5. No cenário de reconciliação direta, observa-se que o protocolo permanece seguro para $T > 0,57$. No cenário de reconciliação reversa, o protocolo permanece seguro para a faixa de valores simulados.

Na sequência foram efetuadas simulações com a espiral de Arquimedes e as curvas geodésicas no toro planar, usando como parâmetros $V_A = 50$ e $\epsilon = 0,0015V_A$ (regra utilizada em [20]). Para a espiral de Arquimedes, as simulações foram realizadas para valores de transmissão na faixa $T \in [0, 1; 1]$. No caso das curvas no toro planar, os valores da transmissão podem ser estendidos para o intervalo $T \in [0,05; 1]$. Quando se trata de uma fibra óptica com

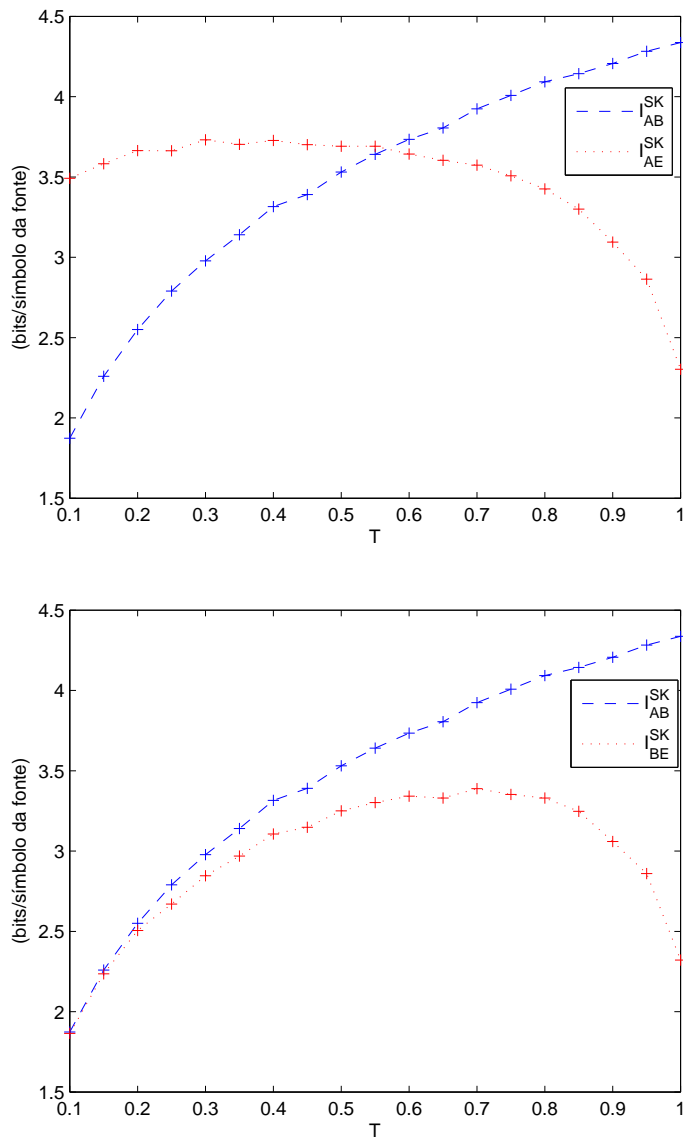


Figura 5.5 No gráfico superior, as informações mútuas I_{AB}^{SK} e I_{AE}^{SK} são comparadas. Pode-se notar que $I_{AB}^{SK} > I_{AE}^{SK}$ para $T > 0,57$. No gráfico inferior, as informações mútuas I_{AB}^{SK} e I_{BE}^{SK} são comparadas. Nota-se que $I_{AB}^{SK} > I_{BE}^{SK}$ para os valores simulados.

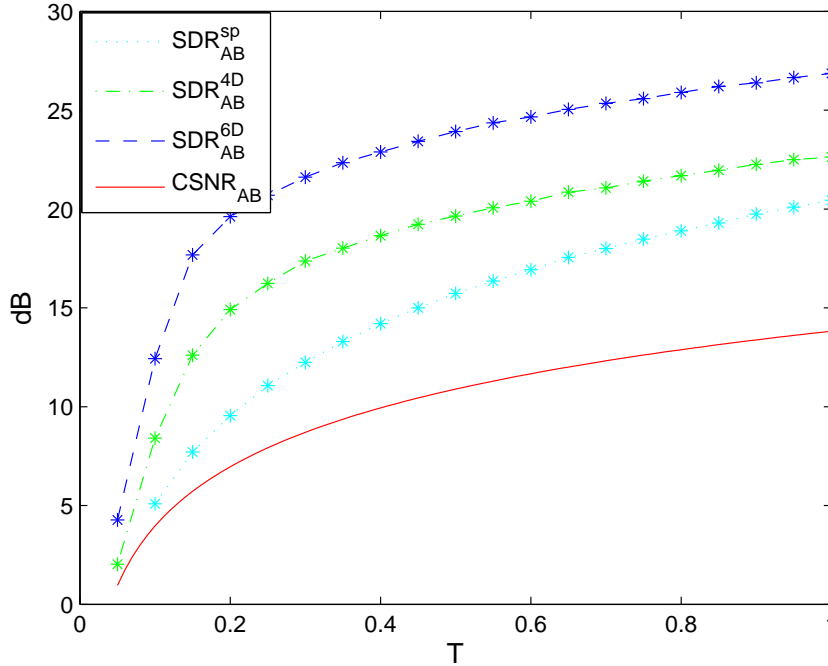


Figura 5.6 Valores simulados para a SDR são comparados a CSNR. O subscrito *sp* se refere à espiral enquanto que *4D* e *6D* se referem à dimensão da curva no toro. É possível notar a tendência de ganhos mais elevados para mapas em dimensões maiores.

atenuação de 0, 2 dB/km, $T = 0, 1$ e $T = 0, 05$ correspondem as distâncias máximas $d = 50$ km e $d = 65$ km, respectivamente. Para as geodésicas no toro planar, foram tomados como base os parâmetros otimizados por [57] e a partir deles foram feitos alguns ajustes no comprimento das curvas através da observação do comportamento da função de raio circular global. Quando $N = 4$, tem-se que $\theta = \{0, 8165; 0, 5773; 0, 7071; 1, 4142\}$ e $L = 7, 74$. Quando $N = 6$, tem-se que $\theta = \{0, 69; 0, 63; 0, 3564; 0, 5584; 1, 1169; 1, 6753\}$ e $L = 10, 2$.

Na Figura 5.6, compara-se a SDR para a espiral e as geodésicas ($N = 4$ e $N = 6$) coma a CSNR para o protocolo NS. É possível notar a tendência de ganhos mais elevados para mapas em dimensões maiores. Além disso, as geodésicas têm um gráfico mais inclinado em regiões de baixa SNR. Para $N = 6$, há um ganho de 3, 3 dB na SDR comparado a CSNR para $T = 0, 05$. Para o mesmo N , quando T é dobrado, o ganho cresce para 8, 47 dB. Na Figura 5.7, são mostrados os gráficos das informações mútuas para os pontos simulados. No geral, os gráficos exibem a mesma tendência que os limitantes para o protocolo NS. Na reconciliação direta, o ponto de 3 dB acontece ao redor de $T = 0, 6$. De modo similar, na reconciliação reversa, $I_{AB}^{SK} > I_{BE}^{SK}$ na faixa simulada. É importante frisar que os valores da informação mútua crescem com a dimensão. Isso é uma consequência direta de ganhos em SNR maiores para dimensões mais altas.

Na Figura 5.8 são mostradas as razões $\beta_{lim}^{DR}(SK)$ e $\beta_{lim}^{RR}(SK)$ para o protocolo proposto. É possível notar que os mapas SK também ajudam Eva a obter mais informação, de modo a exigir o uso de protocolos de reconciliação mais eficientes para um dado T . Para com-

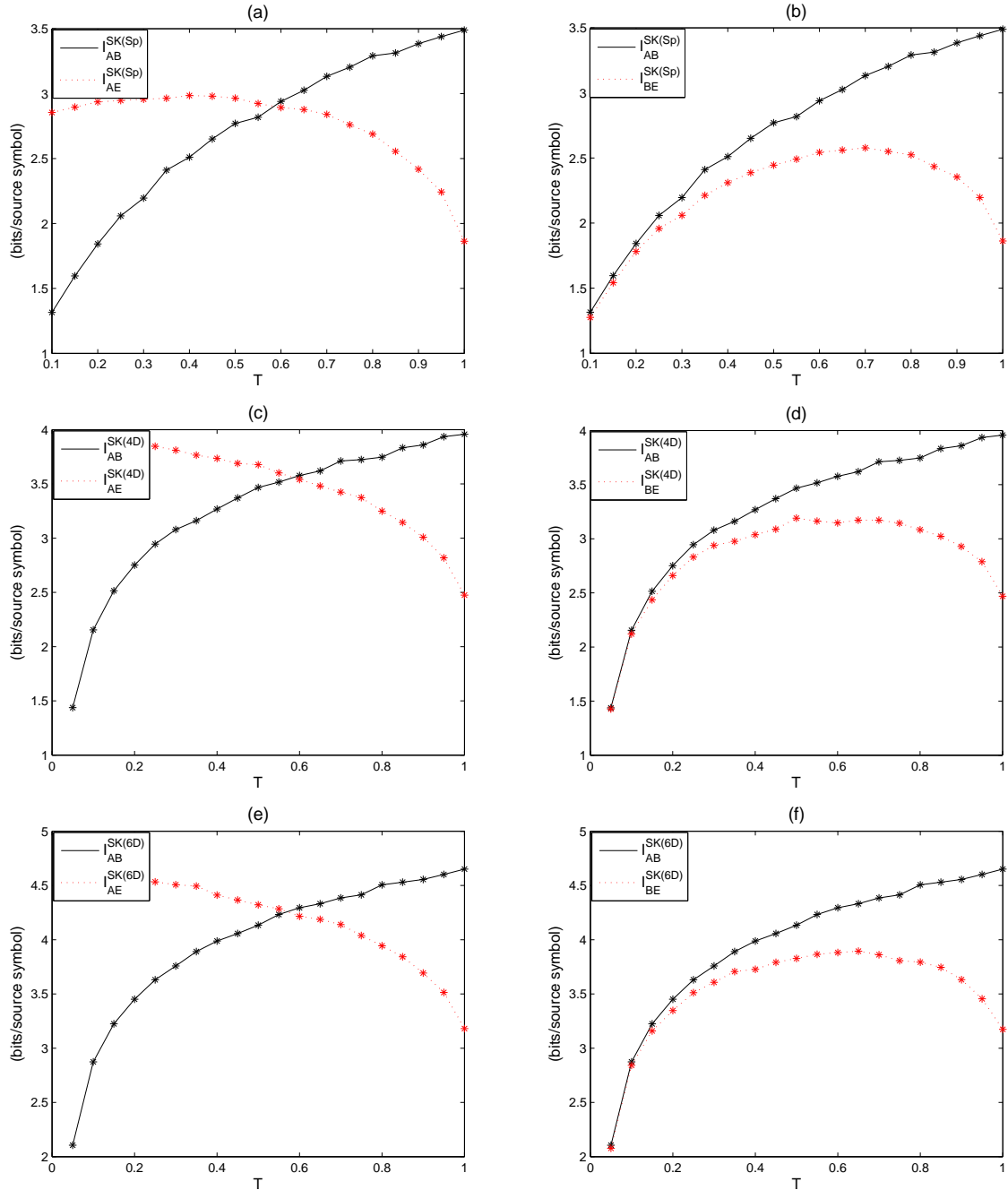


Figura 5.7 Valores simulados para as informações mútuas para o protocolo proposto. No lado esquerdo, é mostrado o caso da reconciliação direta. No lado direito, é mostrado o caso da reconciliação reversa. (a) e (b) foram obtidos para a espiral de Arquimedes. (c),(d) e (e),(f) foram obtidos para as geodésicas no toro planar para $N = 4$ e $N = 6$, respectivamente.

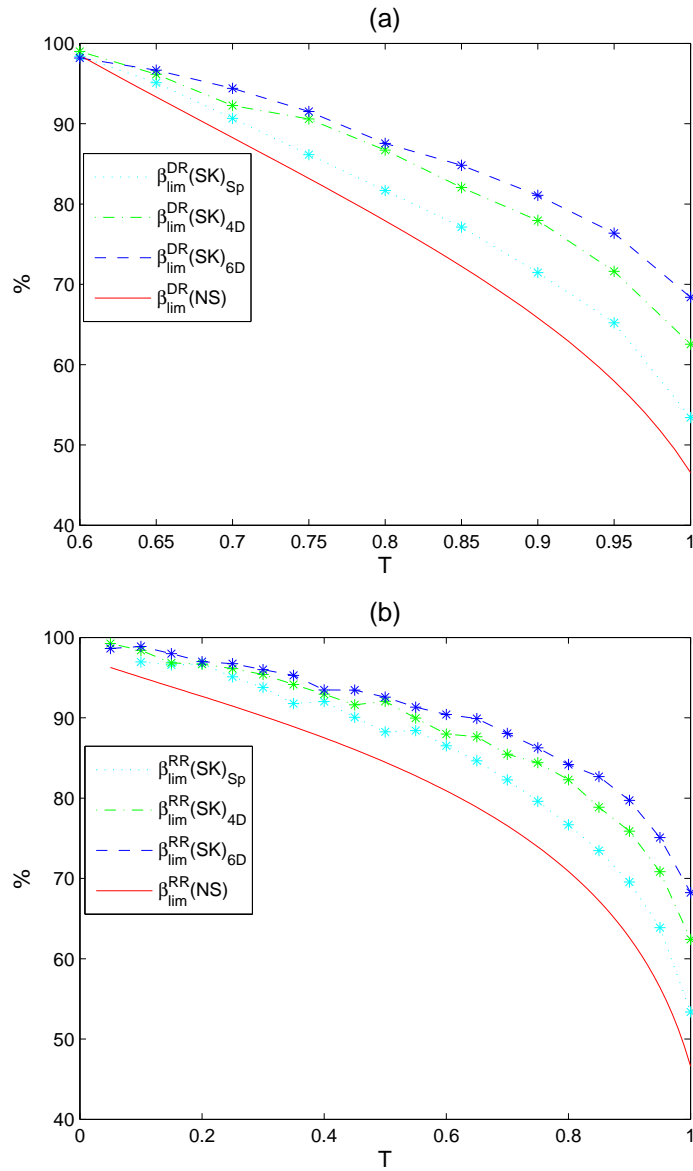


Figura 5.8 Eficiências mínimas de reconciliação são mostradas para a reconciliação direta (a) e reversa (b). Os valores simulados são comparados com o protocolo NS (linhas sólidas vermelhas). É possível notar que o protocolo proposto requer protocolos de reconciliação mais eficientes para um dado T . Esse efeito se torna mais evidente para SNRs mais elevadas.

pensar o crescimento na eficiência de reconciliação, pode-se usar um valor mais baixo para V_A . Para $V_A = 50$, as geodésicas com $N = 6$ requerem $\beta_{lim}^{DR}(SK)_{6D} = 98,6\%$ para uma CSNR = 0,96 dB ($T = 0,05$), resultando em uma SDR = 4,27 dB. Se $V_A = 12,5$ para a mesma CSNR = 0,96 dB (agora $T = 0,20$), ainda se teria uma SDR similar, mas agora com $\beta_{lim}^{DR}(SK)_{6D} = 93,4\%$. Esta nova eficiência requerida é mais baixa que os valores reportados em [20] para esta SNR, de forma que uma chave secreta pode ser extraída para o protocolo proposto a partir dos dados compartilhados. O custo de baixar V_A neste caso foi o crescimento de T (diminuição da distância). A fim de manter os valores de T baixos, poder-se-ia usar mapas de dimensão mais alta como as geodésicas no toro planar para $N = 8$.

CAPÍTULO 6

Conclusões e Perspectivas

Neste trabalho de tese foi proposto um novo protocolo para distribuição quântica de chaves com variáveis contínuas que usa mapeamentos não lineares para a preparação de estados quânticos coerentes. Com a abordagem proposta, foi possível aumentar a SNR entre Alice e Bob através do uso das propriedades de correção de erro dos mapas utilizados. A segurança do protocolo proposto foi avaliada para um ataque do tipo *feedforward*, um ataque individual ótimo para o protocolo NS. As simulações mostraram que a construção proposta realmente aumenta a SNR entre Alice e Bob, além de permitir a extração de uma chave secreta a partir dos dados compartilhados. O lado negativo dessa abordagem é que ela também ajuda Eva a obter mais informação. Este fato é inferido a partir do aumento da eficiência mínima necessária para reconciliação quando comparada ao protocolo NS. Como sugerido no capítulo 6, poder-se-ia baixar a eficiência de reconciliação requerida através da diminuição da variância de Alice combinado com a utilização de mapas de dimensão mais alta.

Como possibilidades de trabalhos futuros, sugere-se:

- Analisar a construção proposta com mapas de dimensões maiores;
- Verificar como o efeito de limiar influencia na eficiência mínima de reconciliação requerida, ou seja, se ele ajuda ou atrapalha as ações de espionagem;
- Incluir nos critérios de projeto dos mapas alguma restrição para confundir Eva, de modo que Eva não obtenha os benefícios do mapeamento;
- Conceber um protocolo que requeira apenas a medição de uma única quadratura a fim de que não se tenha a penalidade quântica da medição de ambas as quadraturas.

Referências Bibliográficas

- [1] Claude E. Shannon. Communication Theory of Secrecy Systems. *Bell Systems Technical Journal*, 28:656–715, 1949.
- [2] Gilles Van Assche. *Quantum Cryptography and Secret-Key Distillation*. Cambridge University Press, 2006.
- [3] William Stallings. *Criptografia e Segurança de Redes*. Prentice Hall Brasil, 2007.
- [4] Simon Singh. *O Livro dos Códigos*. Record, 2010.
- [5] Nicolas Gisin, Grégoire Ribordy, Wolfgang Tittel, and Hugo Zbinden. Quantum cryptography. *Reviews of Modern Physics*, 74:145–195, Mar 2002.
- [6] Nicolas J. Cerf and Philippe Grangier. From quantum cloning to quantum key distribution with continuous variables: a review (invited). *J. Opt. Soc. Am. B*, 24(2):324–334, Feb 2007.
- [7] C. H. Bennett and G. Brassard. Quantum Cryptography: Public Key Distribution and Coin Tossing. In *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing*, pages 175–179, New York, 1984. IEEE Press.
- [8] Charles H. Bennett. Quantum cryptography using any two nonorthogonal states. *Physical Review Letters*, 68:3121–3124, May 1992.
- [9] Artur K. Ekert. Quantum cryptography based on bell’s theorem. *Physical Review Letters*, 67:661–663, Aug 1991.
- [10] Peter W. Shor and John Preskill. Simple proof of security of the bb84 quantum key distribution protocol. *Physical Review Letters*, 85:441–444, Jul 2000.
- [11] Valerio Scarani, Helle Bechmann-Pasquinucci, Nicolas J. Cerf, Miloslav Dušek, Norbert Lütkenhaus, and Momtchil Peev. The security of practical quantum key distribution. *Reviews of Modern Physics*, 81:1301–1350, Sep 2009.

-
- [12] Won-Young Hwang. Quantum key distribution with high loss: Toward global secure communication. *Physical Review Letters*, 91:057901, Aug 2003.
- [13] Hoi-Kwong Lo, Xiongfeng Ma, and Kai Chen. Decoy state quantum key distribution. *Physical Review Letters*, 94:230504, Jun 2005.
- [14] L. Oesterling, D. Hayford, and G. Friend. Comparison of commercial and next generation quantum key distribution: Technologies for secure communication of information. In *Homeland Security (HST), 2012 IEEE Conference on Technologies for*, pages 156–161, Nov 2012.
- [15] Samuel L. Braunstein and Peter van Loock. Quantum information with continuous variables. *Reviews of Modern Physics*, 77:513–577, Jun 2005.
- [16] Christian Weedbrook, Stefano Pirandola, Raul Garcia-Patron, Nicolas J. Cerf, Timothy C. Ralph, Jeffrey H. Shapiro, and Seth Lloyd. Gaussian quantum information. *Reviews of Modern Physics*, 84:621–669, May 2012.
- [17] Yi-Bo Zhao, You-Zhen Gui, Jin-Jian Chen, Zheng-Fu Han, and Guang-Can Guo. Computational complexity of continuous variable quantum key distribution. *Information Theory, IEEE Transactions on*, 54(6):2803–2807, June 2008.
- [18] G. Van Assche, J. Cardinal, and Nicolas J. Cerf. Reconciliation of a quantum-distributed gaussian key. *Information Theory, IEEE Transactions on*, 50(2):394–400, Feb 2004.
- [19] F. Grosshans, G. Van Assche, J. Wenger, R. Brouri, N. J. Cerf, and P. Grangier. Quantum key distribution using gaussian-modulated coherent states. *Nature*, 421:238–241, January 2003.
- [20] Paul Jouguet, David Elkouss, and Sébastien Kunz-Jacques. High-bit-rate continuous-variable quantum key distribution. *Physical Review A*, 90:042329, Oct 2014.
- [21] Jérôme Lodewyck, Matthieu Bloch, Raul García-Patrón, Simon Fossier, Evgueni Karpov, Eleni Diamanti, Thierry Debuisschert, Nicolas J. Cerf, Rosa Tualle-Brouri, Steven W. McLaughlin, and Philippe Grangier. Quantum key distribution over 25 km with an all-fiber continuous-variable system. *Physical Review A*, 76:042305, Oct 2007.
- [22] M. Bloch, A. Thangaraj, S.W. McLaughlin, and J.-M. Merolla. Ldpc-based gaussian key reconciliation. In *Information Theory Workshop, 2006. ITW '06 Punta del Este. IEEE*, pages 116–120, March 2006.
- [23] ZengLiang Bai, XuYang Wang, ShenShen Yang, and YongMin Li. High-efficiency gaussian key reconciliation in continuous variable quantum key distribution. *Science China Physics, Mechanics & Astronomy*, 59(1):1–5, 2016.

-
- [24] Anthony Leverrier, Romain Alléaume, Joseph Boutros, Gilles Zémor, and Philippe Grangier. Multidimensional reconciliation for a continuous-variable quantum key distribution. *Physical Review A*, 77:042325, Apr 2008.
- [25] Paul Jouguet, Sébastien Kunz-Jacques, and Anthony Leverrier. Long-distance continuous-variable quantum key distribution with a gaussian modulation. *Physical Review A*, 84:062317, Dec 2011.
- [26] Paul Jouguet, Sébastien Kunz-Jacques, Anthony Leverrier, Philippe Grangier, and Eleni Diamanti. Experimental demonstration of long-distance continuous-variable quantum key distribution. *Nat Photon*, 7(5):378–381, May 2013.
- [27] S Fossier, E Diamanti, T Debuisschert, R Tualle-Brouri, and P Grangier. Improvement of continuous-variable quantum key distribution systems by using optical preamplifiers. *Journal of Physics B: Atomic, Molecular and Optical Physics*, 42(11):114014, 2009.
- [28] T. C. Ralph and A. P. Lund. Nondeterministic noiseless linear amplification of quantum systems. *AIP Conference Proceedings*, 1110(1):155–160, 2009.
- [29] Rémi Blandino, Anthony Leverrier, Marco Barbieri, Jean Etesse, Philippe Grangier, and Rosa Tualle-Brouri. Improving the maximum transmission distance of continuous-variable quantum key distribution using a noiseless amplifier. *Phys. Rev. A*, 86:012327, Jul 2012.
- [30] Christian Weedbrook, Andrew M. Lance, Warwick P. Bowen, Thomas Symul, Timothy C. Ralph, and Ping Koy Lam. Quantum cryptography without switching. *Physical Review Letters*, 93:170504, Oct 2004.
- [31] Yichen Zhang, Song Yu, and Hong Guo. Application of practical noiseless linear amplifier in no-switching continuous-variable quantum cryptography. *Quantum Information Processing*, 14(11):4339–4349, 2015.
- [32] John M. Wozencraft and Irwin Mark Jacobs. *Principles of Communication Engineering*. John Wiley and Sons, Inc., 1965.
- [33] D. J. Sakrison. *Communication Theory: Transmission of Waveforms and Digital Information*. John Wiley and Sons, Inc., 1968.
- [34] Francisco Revson, Edmar Nascimento, and Francisco M. Assis. Distribuição quântica de chave utilizando modulação não linear. In *XXXIII Simpósio Brasileiro de Telecomunicações 2015 (SBrT2015)*, Juiz de Fora, Brazil, September 2015.
- [35] E. J. Nascimento and F. M. de Assis. Improving continuous-variable quantum key distribution with shannon-kotel’nikov maps. In *2016 IEEE Globecom Workshops (GC Wkshps)*, pages 1–6, Dec 2016.

-
- [36] Ulf Leonhardt. *Essential Quantum Optics: From Quantum Measurements to Black Holes*. Cambridge University Press, 2010.
- [37] J. Perina, Z. Hradil, and B. Jurco. *Quantum Optics and Fundamentals of Physics*. Kluwer Academic Publishers, 1994.
- [38] Christopher Gerry and Peter Knight. *Introductory Quantum Optics*. Cambridge University Press, 2005.
- [39] Mark Fox. *Quantum Optics: An Introduction*. Oxford University Press, 2006.
- [40] Marlan O. Scully and M. Suhail Zubairy. *Quantum Optics*. Cambridge University Press, 1997.
- [41] Leonard Mandel and Emil Wolf. *Optical Coherence and Quantum Optics*. Cambridge University Press, 1995.
- [42] Jérôme Wenger. *Dispositifs impulsions pour la communication quantique à variables continues*. PhD thesis, Université Paris Sud - Paris XI, France, 2004.
- [43] Raúl García-Patrón. *Quantum information with optical continuous variables: from Bell tests to key distribution*. PhD thesis, Université Libre de Bruxelles, Bruxelles, 2007.
- [44] Anthony Leverrier. *Etude théorique de la distribution quantique de clés à variables continues*. PhD thesis, École Nationale Supérieure des Télécommunications, Paris, France, 2009.
- [45] Michael A. Nielsen and Isaac L. Chuang. *Computação Quântica e Informação Quântica*. Bookman, 2005.
- [46] Crispin W. Gardiner. *Quantum Noise*. Springer-Verlag, 1991.
- [47] Henrique Bursztyn and Leonardo Macarini. *Introdução à geometria simplética*. IMPA, 2006.
- [48] Horace P. Yuen and J.H. Shapiro. Optical communication with two-photon coherent states—part iii: Quantum measurements realizable with photoemissive detectors. *Information Theory, IEEE Transactions on*, 26(1):78–92, Jan 1980.
- [49] Thomas M. Cover and Joy A. Thomas. *Elements of Information Theory*. John Wiley and Sons, Inc., New York, 1991.
- [50] F. Hekland, P. A. Floor, and T. A. Ramstad. Shannon-kotel-nikov mappings in joint source-channel coding. *IEEE Transactions on Communications*, 57(1):94–105, January 2009.

-
- [51] P.A. Floor and T.A. Ramstad. Noise analysis for dimension expanding mappings in source-channel coding. In *Signal Processing Advances in Wireless Communications, 2006. SPAWC '06. IEEE 7th Workshop on*, pages 1–5, July 2006.
- [52] John Proakis and Masoud Salehi. *Digital Communications*. McGraw-Hill, 2008.
- [53] T. Goblick. Theoretical limitations on the transmission of data from analog sources. *IEEE Transactions on Information Theory*, 11(4):558–567, Oct 1965.
- [54] J. Ziv. The behavior of analog communication systems. *IEEE Transactions on Information Theory*, 16(5):587–594, Sep 1970.
- [55] V. A. Vaishampayan and S. I. R. Costa. Curves on a sphere, shift-map dynamics, and error control for continuous alphabet sources. *IEEE Transactions on Information Theory*, 49(7):1658–1672, July 2003.
- [56] Sueli I. Rodrigues Costa. On closed twisted curves. *Proceedings of the American Mathematical Society*, 109(1):205–214, May 1990.
- [57] R. M. Taylor, L. Mili, and A. Zaghoul. Packing tubes on tori: An efficient method for low snr analog error correction. In *Information Theory Workshop (ITW), 2013 IEEE*, pages 1–5, Sept 2013.
- [58] Oscar Gonzalez and John H. Maddocks. Global curvature, thickness, and the ideal shapes of knots. *Proceedings of the National Academy of Sciences*, 96(9):4769–4773, 1999.
- [59] F. Grosshans, A. Acín, and N. J. Cerf. *Continuous-Variable Quantum Key Distribution*, chapter 4, pages 63–83.
- [60] R. Renner and J. I. Cirac. de finetti representation theorem for infinite-dimensional quantum systems and applications to quantum cryptography. *Physical Review Letters*, 102:110504, Mar 2009.
- [61] Yi Mu, Jennifer Seberry, and Yuliang Zheng. Shared cryptographic bits via quantized quadrature phase amplitudes of light. *Optics Communications*, 123:344 – 352, 1996.
- [62] T. C. Ralph. Continuous variable quantum cryptography. *Physical Review A*, 61:010303, Dec 1999.
- [63] Mark Hillery. Quantum cryptography with squeezed states. *Physical Review A*, 61:022309, Jan 2000.
- [64] N. J. Cerf, M. Lévy, and G. Van Assche. Quantum distribution of gaussian keys using squeezed states. *Physical Review A*, 63:052311, Apr 2001.

-
- [65] Frédéric Grosshans and Philippe Grangier. Continuous variable quantum cryptography using coherent states. *Physical Review Letters*, 88:057902, Jan 2002.
- [66] Daniel Gottesman and John Preskill. Secure quantum key distribution using squeezed states. *Physical Review A*, 63:022309, Jan 2001.
- [67] N. J. Cerf, A. Ipe, and X. Rottenberg. Cloning of continuous quantum variables. *Physical Review Letters*, 85:1754–1757, Aug 2000.
- [68] Raúl García-Patrón and Nicolas J. Cerf. Unconditional optimality of gaussian attacks against continuous-variable quantum key distribution. *Physical Review Letters*, 97:190503, Nov 2006.
- [69] Christian Weedbrook, Andrew M. Lance, Warwick P. Bowen, Thomas Symul, Timothy C. Ralph, and Ping Koy Lam. Coherent-state quantum key distribution without random basis switching. *Physical Review A*, 73:022316, Feb 2006.
- [70] J. Sudjana, L. Magnin, R. García-Patrón, and N. J. Cerf. Tight bounds on the eavesdropping of a continuous-variable quantum cryptographic protocol with no basis switching. *Physical Review A*, 76:052301, Nov 2007.
- [71] Jérôme Lodewyck and Philippe Grangier. Tight bound on the coherent-state quantum key distribution with heterodyne detection. *Physical Review A*, 76:022332, Aug 2007.
- [72] Yi-Bo Zhao, Matthias Heid, Johannes Rigas, and Norbert Lütkenhaus. Asymptotic security of binary modulated continuous-variable quantum key distribution under collective attacks. *Physical Review A*, 79:012307, Jan 2009.
- [73] Anthony Leverrier and Philippe Grangier. Unconditional security proof of long-distance continuous-variable quantum key distribution with discrete modulation. *Physical Review Letters*, 102:180504, May 2009.
- [74] A. Leverrier and P. Grangier. Continuous-variable Quantum Key Distribution protocols with a discrete modulation. *ArXiv e-prints*, February 2010.
- [75] Peng Huang, Jian Fang, and Guihua Zeng. State-discrimination attack on discretely modulated continuous-variable quantum key distribution. *Physical Review A*, 89:042330, Apr 2014.
- [76] Anthony Leverrier and Philippe Grangier. Continuous-variable quantum-key-distribution protocols with a non-gaussian modulation. *Physical Review A*, 83:042312, Apr 2011.
- [77] Jian Yang, Bingjie Xu, Xiang Peng, and Hong Guo. Four-state continuous-variable quantum key distribution with long secure distance. *Physical Review A*, 85:052302, May 2012.

-
- [78] Ch. Silberhorn, T. C. Ralph, N. Lütkenhaus, and G. Leuchs. Continuous variable quantum cryptography: Beating the 3 db loss limit. *Physical Review Letters*, 89:167901, Sep 2002.
- [79] Denis Sych and Gerd Leuchs. Coherent state quantum key distribution with multi letter phase-shift keying. *New Journal of Physics*, 12(5):053019, 2010.
- [80] Ryo Namiki and Takuya Hirano. Efficient-phase-encoding protocols for continuous-variable quantum key distribution using coherent states and postselection. *Physical Review A*, 74:032302, Sep 2006.
- [81] Zhengyu Li, Yi-Chen Zhang, Feihu Xu, Xiang Peng, and Hong Guo. Continuous-variable measurement-device-independent quantum key distribution. *Physical Review A*, 89:052301, May 2014.
- [82] Yi-Chen Zhang, Zhengyu Li, Song Yu, Wanyi Gu, Xiang Peng, and Hong Guo. Continuous-variable measurement-device-independent quantum key distribution using squeezed states. *Physical Review A*, 90:052325, Nov 2014.
- [83] D. Slepian and J.K. Wolf. Noiseless coding of correlated information sources. *Information Theory, IEEE Transactions on*, 19(4):471–480, Jul 1973.
- [84] Gilles Brassard and Louis Salvail. Secret-key reconciliation by public discussion. In Tor Helleseth, editor, *Advances in Cryptology - EUROCRYPT 93*, volume 765 of *Lecture Notes in Computer Science*, pages 410–423. Springer Berlin Heidelberg, 1994.
- [85] Shu Lin and Daniel Costello. *Error Control Coding: Fundamentals and Applications*. Prentice Hall, 1983.
- [86] M. Bloch, A. Thangaraj, S.W. McLaughlin, and J.-M. Merolla. Ldpc-based secret key agreement over the gaussian wiretap channel. In *Information Theory, 2006 IEEE International Symposium on*, pages 1179–1183, July 2006.
- [87] M. Bloch, A. Thangaraj, and S. W. McLaughlin. Efficient Reconciliation of Correlated Continuous Random Variables using LDPC Codes. *eprint arXiv:cs/0509041*, September 2005.
- [88] C.H. Bennett, G. Brassard, C. Crepeau, and U.M. Maurer. Generalized privacy amplification. *Information Theory, IEEE Transactions on*, 41(6):1915–1923, 1995.
- [89] J.Lawrence Carter and Mark N. Wegman. Universal classes of hash functions. *Journal of Computer and System Sciences*, 18(2):143 – 154, 1979.
- [90] Alexander Kraskov, Harald Stögbauer, and Peter Grassberger. Estimating mutual information. *Physical Review E*, 69:066138, Jun 2004.

APÊNDICE A

Lista de Artigos Produzidos

Segue abaixo a lista de artigos produzidos ao longo deste trabalho de tese.

- [1] Edmar J. Nascimento e Francisco M. de Assis, “Enhancing continuous-variable quantum key distribution by state preparation with Shannon-Kotel’nikov maps,” Submetido para a revista *Quantum Information Processing (Springer)*.
- [2] Edmar J. Nascimento e Francisco M. de Assis, “Improving Continuous-Variable Quantum Key Distribution with Shannon-Kotel’nikov Maps”, In: *2016 IEEE Globecom Workshops (GC Wkshps)*, Washington-DC, USA, 2016.
- [3] F. R. F. Pereira, E. J. Nascimento e F. M. de Assis, “Distribuição Quântica de Chave Utilizando Modulação Não Linear”, In: *XXXIII Simpósio Brasileiro de Telecomunicações (SBRT2015)*, Juiz de Fora-MG, 2015.
- [4] E. J. Nascimento e F. M. Assis, “Análise dos protocolos para distribuição quântica de chaves usando variáveis contínuas”, In: *V Workshop Escola em Computação e Informação Quânticas (V WeciQ)*, Campina Grande-PB, 2015.

APÊNDICE B

Código Fonte das Simulações

B.1 Espiral Uniforme de Arquimedes

```
% Shannon–Kotel'nikov Map for state preparation
% Archimedes' spiral

% General settings

NInt = 100000; % Number of iterations
nSIntervals = 1000; % Number of source intervals
VA = 50; % Alice's variance in Shot Noise (SN) units
% Quantum channel
P = VA; % Input channel power
T = 0.05; % Transmission [0,1] – to be varied
e = 0.075; % Excess noise 0.0015*VA
X = (1-T)./T + e;
gE = sqrt(e*T); % Feedforward Attack
TE = 4*(2-sqrt(e*(2-2*T+T*e)))./(((2+T*e).^2)./T) - T*(2-e)/(2+T*e);
% Spiral
CSNRdBdes = 10*log10(0.5*T*VA/(2+T*e)) % CSNR for designing the spiral
DeltaOp = sqrt(P)*5.223*exp(-((3e-4)*CSNRdBdes^2 + 0.0801*CSNRdBdes));
Delta = DeltaOp; % Distance between two spiral arms
sigma_x = 0.25; % Source standard deviation
eta = 0.16;
alpha = P*eta*sqrt(2*pi^5)/(Delta*sigma_x*(1-exp(-1/(2*sigma_x^2))));

% Source (Discretization for ML decoding)

domain_x = -1:2/nSIntervals:1; % Source domain (truncated to [-1,1])
phiSource = sqrt(abs(alpha*domain_x/(eta*Delta)));
sxSource = Delta/pi*[sign(domain_x).*phiSource.*cos(phiSource);...
    sign(domain_x).*phiSource.*sin(phiSource)]; % Source mapping
[mx,nx] = size(sxSource);
```

```

% Encoding (Generation of source symbols and mapping)
xSim = sigma_x*randn([1,NInt]); % Source symbols
countSat = 0; % Source saturating events (statistical purposes)
for n = 1:NInt % Truncation
    if xSim(n) > 1
        xSim(n)=1;
        countSat = countSat+1;
    end
    if xSim(n) < -1
        xSim(n)=-1;
        countSat = countSat+1;
    end
end
phiSourceSim = sqrt(abs(alpha*xSim/(eta*Delta)));
sxSourceSim = Delta/pi*[sign(xSim).*phiSourceSim.*cos(phiSourceSim);...
    sign(xSim).*phiSourceSim.*sin(phiSourceSim)];% Source mapping
xpa = sxSourceSim; % Alice's quadrature displacements
vxpa = [xpa(1,:); xpa(2,:)]; % Alice's quadrature displacements in a vector
dxea = randn(2,NInt); % Alice's shot noise
alpha_Alice = xpa + dxpa; % Alice's coherent states

% Channel
% Eve (Feedforward attack)
bs_sn_TE = randn(2,NInt); % Eve's beam splitter shot noise
xp_TE = sqrt(TE)*(alpha_Alice) + sqrt(1-TE)*bs_sn_TE; % Transmitted
xp_RefE = -sqrt(1-TE)*(alpha_Alice) + sqrt(TE)*bs_sn_TE; % Reflected
bs_sn_ME = randn(2,NInt); % Eve's beam splitter shot noise
xp_ME = sqrt(1/2)*[xp_RefE(1,:) + bs_sn_ME(1,:);...
    -xp_RefE(2,)+ bs_sn_ME(2,:)]; % Eve's measured quadratures
alpha_Bob = [-gE*xp_ME(1,:);gE*xp_ME(2,:)] + xp_TE; % Channel output

% Bob
bs_sn = randn(2,NInt); % Bob's measurement noise
xpb = sqrt(1/2)*[alpha_Bob(1,:) + bs_sn(1,:);...
    -alpha_Bob(2,)+ bs_sn(2,:)]; % Bob's measured quadratures

% Parameter estimation (Debug)
VAx_est = sum(xpa(1,:).^2)/NInt;
VAp_est = sum(xpa(2,:).^2)/NInt;
VBx_est = sum(xpb(1,:).^2)/NInt;
Vbp_est = sum(xpb(2,:).^2)/NInt;
Tx_est = 2*(sum(xpb(1,).*xpa(1,))/NInt)^2/(VAx_est)^2;
Tp_est = 2*(sum(xpb(2,).*xpa(2,))/NInt)^2/(VAp_est)^2;
ex_est = 2*(VBx_est-1)/Tx_est - VAx_est;
ep_est = 2*(Vbp_est-1)/Tp_est - VAp_est;
Xx_est = (1-Tx_est)./Tx_est + ex_est;

```

```

Xp_est = (1-Tp_est)./Tp_est + ep_est;

% Quadratures for ML decoding
vxpb = [sqrt(2/Tx_est)*xpb(1,:), -sqrt(2/Tp_est)*xpb(2,:)];
vxpe = [-sqrt(2/(1-TE))*xp_ME(1,:), sqrt(2/(1-TE))*xp_ME(2,:)];

% ML Decoding (Bob)
indexDec = zeros(1,NInt);
for n = 1:NInt
    sDec = [vxpb(1,n)*ones(1,nx); vxpb(2,n)*ones(1,nx)];
    diff = sDec - sxSource;
    distance = sqrt(sum(diff.^2,1));
    [dMin,ind] = min(distance);
    indexDec(n) = ind;
end
xDec = domain_x(indexDec);

% ML Decoding (Eve)
indexDecE = zeros(1,NInt);
for n = 1:NInt
    sDecE = [vxpe(1,n)*ones(1,nx); vxpe(2,n)*ones(1,nx)];
    diff = sDecE - sxSource;
    distance = sqrt(sum(diff.^2,1));
    [dMin,ind] = min(distance);
    indexDecE(n) = ind;
end
eDec = domain_x(indexDecE);

% Results
% MSE
MSEAB = sum((xDec-xSim).^2)/(NInt);
MSEAE = sum((eDec-xSim).^2)/(NInt);
MSEBE = sum((eDec-xDec).^2)/(NInt);
% SDR
SNRAB = sigma_x^2/MSEAB;
SNRAE = sigma_x^2/MSEAE;
SNRBE = sigma_x^2/MSEBE;
SNRdBAB = 10*log10(SNRAB);
SNRdBAE = 10*log10(SNRAE);
SNRdBBE = 10*log10(SNRBE);

CSNR = T*VA/(2+T*e); % CSNR for the NS protocol
CSNRdB = 10*log10(CSNR);
gain = SNRAB/CSNR;
% Kraskov's estimator
[IMAMB1,IMAMB2] = KraskovMI(xSim(1:10000)',...
    xDec(1:10000)'+1e-9*randn(1,10000)',5); % Only 10^4 samples are used

```

```
[IMAME1,IMAME2] = KraskovMI(xSim(1:10000)',...
    eDec(1:10000)'+1e-9*randn(1,10000)',5);
[IMBME1,IMBME2] = KraskovMI(xDec(1:10000)'+1e-9*randn(1,10000)',...
    eDec(1:10000)'+1e-9*randn(1,10000)',5);
```

```
% Key rates
```

```
DI_DR = IMAMB1-IMAME1;
```

```
DI_RR = IMAMB1-IMBME1;
```

```
beta_lim_DR = IMAME1/IMAMB1; % Just make sense above 3dB limit
```

```
beta_lim_RR = IMBME1/IMAMB1;
```

B.2 Geodésicas no Toro Planar $N = 4$

```
% Shannon-Kotel'nikov Map for state preparation
```

```
% Geodesics on a flat torus
```

```
% N = 4 (Number of dimensions)
```

```
% General settings
```

```
NInt = 100000; % Number of points in the simulation
```

```
nSIntervals = 20000; % Number of source intervals
```

```
VA = 50; % Alice's variance in Shot Noise (SN) units
```

```
% Quantum channel
```

```
T = 1.00; % Transmission [0,1] - to be varied
```

```
e = 0.0015*VA; % Excess noise 0.0015*VA
```

```
N = 4; % Channel dimension
```

```
Pin = N*VA; % Input channel power
```

```
X = (1-T)./T + e;
```

```
gE = sqrt(e*T); % Feedforward Attack
```

```
TE = 4*(2-sqrt(e*(2-2*T+T*e)))./(((2+T*e).^2)./T) - T*(2-e)./(2+T*e);
```

```
% Geodesic parameters
```

```
% L = 7.6; % Curve length (article)
```

```
L = 7.74; % Adjusted by visual observation of global circumradius function
```

```
r1 = 0.8165; % Curve parameters
```

```
r2 = 0.5773;
```

```
om1 = 0.7071;
```

```
om2 = 1.4142;
```

```
% Source
```

```
a = -1; % Source interval [a,b]
```

```
b = 1;
```

```
sigma_s = 0.25; % Source standard deviation
```

```
Ps = sigma_s^2; % Average source power
```

```
% Source (Discretization for ML decoding)
```

```
syms u x real
```

```

fs = 1/sqrt(2*pi*sigma_s^2)*exp(-(u.^2)/(2*sigma_s^2)); % Source pdf
fs13 = (1/sqrt(2*pi*sigma_s^2))^(1/3)*exp(-(u.^2)/(6*sigma_s^2));% fs^(1/3)
den = int(fs13,u,-1,1); % Symbolic
num = int(fs13,u,-1,x); % Symbolic
s_gauss = a:(b-a)/nSIntervals:b; % Support of the source s~[a,b]
s = 2*subs(num,x,s_gauss)/double(den)-1; % Compander
alpha_s = L*s/2; % Stretching
x_alpha_s = sqrt(Pin)*[r1*cos(om1*alpha_s);r1*sin(om1*alpha_s);...
    r2*cos(om2*alpha_s);r2*sin(om2*alpha_s)]; % Curve - points in columns
[mx,nx] = size(x_alpha_s);

% Encoding (Generation of source symbols and mapping)
sSim = sigma_s*randn([1,NInt]); % Source symbols
countSat = 0; % Source saturating events (statistical purposes)
for n = 1:NInt % Truncation
    if sSim(n) > 1
        sSim(n)=1;
        countSat = countSat+1;
    end
    if sSim(n) < -1
        sSim(n)=-1;
        countSat = countSat+1;
    end
end
end
varsSim = sum(sSim.^2)/NInt - (sum(sSim)/NInt)^2;
sSimCompanding = 2*subs(num,x,sSim)/double(den)-1; % Compander
alpha_sSim = L*sSimCompanding/2; % Stretching
x_Sim = sqrt(Pin)*[r1*cos(om1*alpha_sSim);r1*sin(om1*alpha_sSim);...
    r2*cos(om2*alpha_sSim);r2*sin(om2*alpha_sSim)]; % Source mapping
xpa1 = x_Sim(1:2,:); % Alice's quadrature displacements
xpa2 = x_Sim(3:4,:); % Alice's quadrature displacements
vxpa1 = [xpa1(1,:); xpa1(2,:)]; % Alice's quadrature displacements
vxpa2 = [xpa2(1,:); xpa2(2,:)]; % Alice's quadrature displacements
dxxpa1 = randn(2,NInt); % Alice's shot noise
dxxpa2 = randn(2,NInt); % Alice's shot noise
alpha_Alice1 = xpa1 + dxxpa1; % Alice's first coherent state
alpha_Alice2 = xpa2 + dxxpa2; % Alice's second coherent state

% Channel
% Eve (Feedforward attack)
bs_sn_TE1 = randn(2,NInt); % Eve's beam splitter shot noise
bs_sn_TE2 = randn(2,NInt); % Eve's beam splitter shot noise
xp_TE1 = sqrt(TE)*(alpha_Alice1) + sqrt(1-TE)*bs_sn_TE1; % Transmitted
xp_TE2 = sqrt(TE)*(alpha_Alice2) + sqrt(1-TE)*bs_sn_TE2; % Transmitted
xp_RefE1 = -sqrt(1-TE)*(alpha_Alice1) + sqrt(TE)*bs_sn_TE1; % Reflected
xp_RefE2 = -sqrt(1-TE)*(alpha_Alice2) + sqrt(TE)*bs_sn_TE2; % Reflected
bs_sn_ME1 = randn(2,NInt); % Eve's beam splitter shot noise

```

```

bs_sn_ME2 = randn(2,NInt); % Eve's beam splitter shot noise
xp_ME1 = sqrt(1/2)*[xp_RefE1(1,:) + bs_sn_ME1(1,:);...
    -xp_RefE1(2,)+ bs_sn_ME1(2,:)]; % Eve's measured quadratures
xp_ME2 = sqrt(1/2)*[xp_RefE2(1,:) + bs_sn_ME2(1,:);...
    -xp_RefE2(2,)+ bs_sn_ME2(2,:)]; % Eve's measured quadratures
alpha_Bob1 = [-gE*xp_ME1(1,:);gE*xp_ME1(2,:)] + xp_TE1; % Channel output
alpha_Bob2 = [-gE*xp_ME2(1,:);gE*xp_ME2(2,:)] + xp_TE2; % Channel output

% Bob
bs_sn1 = randn(2,NInt); % Bob's measurement noise
bs_sn2 = randn(2,NInt); % Bob's measurement noise
xpb1 = sqrt(1/2)*[alpha_Bob1(1,:) + bs_sn1(1,:);...
    -alpha_Bob1(2,)+ bs_sn1(2,:)]; % Bob's measured quadratures
xpb2 = sqrt(1/2)*[alpha_Bob2(1,:) + bs_sn2(1,:);...
    -alpha_Bob2(2,)+ bs_sn2(2,:)]; % Bob's measured quadratures

% Parameter estimation (Debug)
% Alice
VAX_est1 = sum(xpa1(1,:).^2)/NInt; % Alice's estimated variance x
VAp_est1 = sum(xpa1(2,:).^2)/NInt; % Alice's estimated variance p
VAX_est2 = sum(xpa2(1,:).^2)/NInt; % Alice's estimated variance x
VAp_est2 = sum(xpa2(2,:).^2)/NInt; % Alice's estimated variance p
VA_est = VAX_est1 + VAp_est1 + VAX_est2 + VAp_est2 % Alice's total variance
VA_est_av = VA_est/N % Alice's average variance
% Bob
VBX_est1 = sum(xpb1(1,:).^2)/NInt; % Bob's estimated variance x
VBP_est1 = sum(xpb1(2,:).^2)/NInt; % Bob's estimated variance p
VBX_est2 = sum(xpb2(1,:).^2)/NInt; % Bob's estimated variance x
VBP_est2 = sum(xpb2(2,:).^2)/NInt; % Bob's estimated variance p
VB_est = VBX_est1 + VBP_est1 + VBX_est2 + VBP_est2; % Bob's total variance
%Channel
Tx_est1 = 2*(sum(xpb1(1,:).*xpa1(1,:))/NInt)^2/(VAX_est1)^2; % T estimate
Tp_est1 = 2*(sum(xpb1(2,:).*xpa1(2,:))/NInt)^2/(VAp_est1)^2; % T estimate
ex_est1 = 2*(VBX_est1-1)/Tx_est1 - VAX_est1; % e estimate
ep_est1 = 2*(VBP_est1-1)/Tp_est1 - VAp_est1; % e estimate
Xx_est1 = (1-Tx_est1)./Tx_est1 + ex_est1;
Xp_est1 = (1-Tp_est1)./Tp_est1 + ep_est1;
Tx_est2 = 2*(sum(xpb2(1,:).*xpa2(1,:))/NInt)^2/(VAX_est2)^2; % T estimate
Tp_est2 = 2*(sum(xpb2(2,:).*xpa2(2,:))/NInt)^2/(VAp_est2)^2; % T estimate
ex_est2 = 2*(VBX_est2-1)/Tx_est2 - VAX_est2; % e estimate
ep_est2 = 2*(VBP_est2-1)/Tp_est2 - VAp_est2; % e estimate
Xx_est2 = (1-Tx_est2)./Tx_est2 + ex_est2;
Xp_est2 = (1-Tp_est2)./Tp_est2 + ep_est2;

% Quadratures for ML decoding
% Bob
vxpb1 = [sqrt(2/Tx_est1)*xpb1(1,:); -sqrt(2/Tp_est1)*xpb1(2,:)];

```

```

vxpb2 = [sqrt(2/Tx_est2)*xpb2(1,:); -sqrt(2/Tp_est2)*xpb2(2,:)];
% Eve
vxpe1 = [-sqrt(2/(1-TE))*xp_ME1(1,:); sqrt(2/(1-TE))*xp_ME1(2,:)];
vxpe2 = [-sqrt(2/(1-TE))*xp_ME2(1,:); sqrt(2/(1-TE))*xp_ME2(2,:)];

% ML Decoding (Bob)
indexDec = zeros(1,NInt);
for n = 1:NInt
    y_Dec = [vxpb1(1,n)*ones(1,nx); vxpb1(2,n)*ones(1,nx); ...
            vxpb2(1,n)*ones(1,nx); vxpb2(2,n)*ones(1,nx)];
    diff = y_Dec - x_alpha_s;
    distance = sqrt(sum(diff.^2,1));
    [dMin,ind] = min(distance);
    indexDec(n) = ind;
end
sDec = s_gauss(indexDec);

% ML Decoding (Eve)
indexDecE = zeros(1,NInt);
for n = 1:NInt
    sDecE = [vxpe1(1,n)*ones(1,nx); vxpe1(2,n)*ones(1,nx); ...
            vxpe2(1,n)*ones(1,nx); vxpe2(2,n)*ones(1,nx)];
    diff = sDecE - x_alpha_s;
    distance = sqrt(sum(diff.^2,1));
    [dMin,ind] = min(distance);
    indexDecE(n) = ind;
end
eDec = s_gauss(indexDecE);

% Results
errSource = varsSim - Ps;
% MSE
MSEAB = sum((sDec-sSim).^2)/(NInt);
MSEAE = sum((eDec-sSim).^2)/(NInt);
MSEBE = sum((eDec-sDec).^2)/(NInt);
% SDR
SNRAB = varsSim/MSEAB;
SNRAE = varsSim/MSEAE;
SNRBE = varsSim/MSEBE;
SNRdBAB = 10*log10(SNRAB);
SNRdBAE = 10*log10(SNRAE);
SNRdBBE = 10*log10(SNRBE);

CSNR = T*VA/(2+T*e); % CSNR for the NS protocol
CSNRdB = 10*log10(CSNR);
gain = SNRAB/CSNR;
gaindB = SNRdBAB - CSNRdB;

```

```

% Kraskov's estimator
[IMAMB1,IMAMB2] = KraskovMI(sSim(1:10000)',...
    sDec(1:10000)'+1e-9*randn(1,10000)',5); % Only 10^4 samples are used
[IMAME1,IMAME2] = KraskovMI(sSim(1:10000)',...
    eDec(1:10000)'+1e-9*randn(1,10000)',5);
[IMBME1,IMBME2] = KraskovMI(sDec(1:10000)'+1e-9*randn(1,10000)',...
    eDec(1:10000)'+1e-9*randn(1,10000)',5);

% Key rates
DI_DR = IMAMB1-IMAME1;
DI_RR = IMAMB1-IMBME1;

beta_lim_DR = IMAME1/IMAMB1; % Just make sense above 3dB limit
beta_lim_RR = IMBME1/IMAMB1;

```

B.3 Estimador de Kraskov

```

function [ I1, I2 ] = KraskovMI( X, Y, k, varargin )
%KraskovMI computes the Kraskov estimator for the mutual information.
% 1. Input: X, Y
%           k: nearest neighbour
%           zeroFix (optional): fix the negative estimation to 0 (default
%                               false);
%
% univariate: X, Y (n x 1) vector
% multivariate: X, Y (n x m) matrix (rows=observations,
% columns=variables)
%
% 2. Output: I1, I2: the two estimator of MI, I(1), I(2) (see Ref.)
%
% Ref: Kraskov, Alexander, Harald Stögbauer, and Peter Grassberger.
% "Estimating mutual information." Physical review E 69.6 (2004):066138.
%
% Author: Paolo Inglese <paolo.ingls@gmail.com>
% Last revision: 17-05-2015

if nargin < 3 || nargin > 4
    error('Wrong_input_number. ');
end
if nargin == 3
    zeroFix = false;
end
if nargin == 4
    if ~islogical(varargin{1})
        error('zeroFix_must_be_true_or_false ');
    else

```

```

        zeroFix = varargin{1};
    end
end

if size(X, 1) ~= size(Y, 1)
    error('X and Y must contain the same number of samples');
end

nObs = size(X, 1);

% compute distance between each sample and its k-th nearest neighbour
dz = zeros(nObs, nObs);
dx = zeros(nObs, nObs);
dy = zeros(nObs, nObs);
for i = 1:nObs
    for j = 1:nObs
        dx(i, j) = sqrt(sum((X(i, :) - X(j, :)).^2));
        dy(i, j) = sqrt(sum((Y(i, :) - Y(j, :)).^2));
        dz(i, j) = max([dx(i, j), dy(i, j)]);
    end
end

% find nx(i) and ny(i)
Eps = zeros(nObs, 1);
Nn = zeros(nObs, 1);

nx1 = zeros(nObs, 1);
ny1 = zeros(nObs, 1);
nx2 = zeros(nObs, 1);
ny2 = zeros(nObs, 1);
for i = 1:nObs

    dxSample = dx(i, :);
    dxSample(i) = [];

    dySample = dy(i, :);
    dySample(i) = [];

    dzSample = dz(i, :);
    dzSample(i) = [];
    [EpsSample, NnSample] = sort(dzSample, 'ascend');
    Eps(i) = EpsSample(k);
    Nn(i) = NnSample(k);

    nx1(i) = sum(dxSample < Eps(i));
    ny1(i) = sum(dySample < Eps(i));

```

```
nx2(i) = sum(dxSample <= Eps(i));  
ny2(i) = sum(dySample <= Eps(i));
```

```
end
```

```
% mutual information estimators
```

```
I1 = psi(k) - sum(psi(nx1 + 1) + psi(ny1 + 1)) / nObs + psi(nObs);  
I2 = psi(k) - 1/k - sum(psi(nx2) + psi(ny2)) / nObs + psi(nObs);
```

```
if (zeroFix)
```

```
  if I1 < 0
```

```
    warning('First_estimator_is_negative->0');
```

```
    I1 = 0;
```

```
  end
```

```
  if I2 < 0
```

```
    warning('Second_estimator_is_negative->0');
```

```
    I2 = 0;
```

```
  end
```

```
end
```

```
end
```