UNIVERSIDADE FEDERAL DE SÃO CARLOS
CENTRO DE CIÊNCIAS EXATAS E DE TECNOLOGIA
PROGRAMA DE PÓS-GRADUAÇÃO EM FÍSICA

Comunicação Quântica baseada no Teletransporte em Variáveis Contínuas

Fabrício de Souza Luiz

São Carlos
Dezembro/2014

UNIVERSIDADE FEDERAL DE SÃO CARLOS
CENTRO DE CIÊNCIAS EXATAS E DE TECNOLOGIA
PROGRAMA DE PÓS-GRADUAÇÃO EM FÍSICA

Comunicação Quântica baseada no Teletransporte em Variáveis Contínuas

Fabrício de Souza Luiz

Prof. Dr. Gustavo Garcia Rigolin

Tese submetida ao Departamento de Física da
Universidade Federal de São Carlos-DF/UFSCar,
como parte dos requisitos necessários para
obtenção do título de Doutor em Física.

São Carlos
Dezembro/2014

Ficha catalográfica elaborada pelo DePT da Biblioteca Comunitária/UFSCar

L953cq

Luiz, Fabrício de Souza.
Comunicação quântica baseada no teletransporte em variáveis contínuas / Fabrício de Souza Luiz. -- São Carlos : UFSCar, 2014.
136 f.

Tese (Doutorado) -- Universidade Federal de São Carlos, 2014.

1. Física quântica. 2. Teletransporte. 3. Variáveis contínuas. 4. Canal. I. Título.

CDD: 539 (20ª)

UNIVERSIDADE FEDERAL DE SÃO CARLOS

Centro de Ciências Exatas e de Tecnologia
Programa de Pós-Graduação em Física

Folha de Aprovação

Assinaturas dos membros da comissão examinadora que avaliou e aprovou a Defesa de Tese de Doutorado do candidato Fabricio de Souza Luiz, realizada em 12/12/2014:

Prof. Dr. Gustavo Garcia Rigolin
UFSCar

Prof. Dr. Thiago Rodrigues de Oliveira
UFF

Prof. Dr. Salomon Sylvain Mizrahi
UFSCar

Prof. Dr. Miled Hassan Youssef Moussa
USP

Prof. Dr. José Antonio Roversi
UNICAMP

Agradecimentos

Como toda produção científica, essa Tese contou com inúmeras contribuições. Sejam contribuições na forma de incetivo para que eu continuasse trilhando esse caminho, ou em profundas discussões físicas que contribuíram para o meu entendimento da mesma. Dentre essas contribuições, devo destacar as de Márcia de Souza Luiz e Lazaro Antônio Luiz, meus pais. Literalmente, sem eles eu não estaria aqui e também devo agradecê-los pela confiança, incentivos e por acreditarem em mim. Agradeço também a minha namorada, Alessandra Gonçalves Felipe, tenho certeza que sem o seu amor, carinho e compreensão eu não conseguiria.

Devo um agradecimento especial ao Prof. Dr. Gustavo Rigolin, meu orientador, que me guiou nessa jornada científica e é o modelo de cientista que quero me tornar. Quero agradecer o meu amigo Helio Tsuzuki que me amparou em meus momentos de necessidade, ao meu amigo Fabiano Oliveira Prado pela ajuda solícita em meus momentos de necessidade. Aos meus amigos, Thiago Werlang de Oliveira, Daniel Zini Rossatto e Prof. Dr. Celso Jorge Villas-Bôas pelas discussões sobre óptica quântica e seus desdobramentos.

Devo um agradecimento aos meus amigos de longa data, Heitor de Barros falcão e Halyne Silva Borges por me aturarem por tanto tempo. E aos professores do Departamento de Física da UFSCAR pelos seus ensinamentos e aos funcionários do departamento, que durante esses anos contribuíram de algum modo para o meu enriquecimento pessoal e profissional. Gostaria também de agradecer a todos os meus amigos que me incentivaram, alguns de longa data outros mais recentes, porém igualmente importantes, obrigado a todos. Em especial quero agradecer à minha irmã Fabiane de Souza Luiz e à minha sobrinha Anna Luisa de Souza Oliveira.

Finalmente, agradeço ao Conselho Nacional de Pesquisa e Desenvolvimento Cientifico e Tecnológico (CNPq) por ter financiado, nestes quatro anos, meus estudos de doutoramento.

Resumo

Nesta Tese estudamos em detalhes uma das aplicações da mecânica quântica que mais destoa de nosso senso comum: o teletransporte quântico em variáveis Contínuas. Apresentamos uma revisão dos postulados da mecânica quântica e dos sistemas da óptica quântica, em especial sistemas que realizam operações Gaussianas. Após essa revisão aplicamos esses postulados no que resulta na aplicação mais contra intuitiva da mecânica quântica, o teletransporte quântico. Estudamos com detalhes o protocolo de teletransporte e propomos modificações em sua construção visando maximizar a sua eficiência. Estas modificações foram feitas a fim de levar em conta as situações realistas encontradas em sua implementação, qual sejam, o fato de o emaranhamento entre Alice e Bob nunca ser perfeito e o fato de que os estados teletransportados por Alice estarem próximos do estado de vácuo. Após essa análise realizamos uma extensão do protocolo de teletransporte em variáveis contínuas propondo um protocolo de multicanais e estudamos em detalhes o caso de dois canais em paralelo. Por fim, criamos o primeiro protocolo de criptografia quântica que utiliza o teletransporte em variáveis contínuas de forma ativa. Mostramos que esse protocolo é robusto ao ataque de divisor de feixes, sendo o único que funciona com reconciliação direta e sem a necessidade de pós-seleção para perdas superiores a 50%.

Abstract

In this Thesis we study in details one of the most astonishing application of quantum mechanics which totally departs from our common sense: quantum teleportation in continuous variables. We present a review of the postulates of quantum mechanics and quantum optics systems, in particular for Gaussian systems. After this review we apply these postulates in order to present one of the most counter intuitive applications of quantum mechanics, namely, the quantum teleportation protocol. We study in detail this protocol and we propose modifications in its construction aiming at an improvement in its efficiency. These modifications were made in order to take into account the realistic situations encountered in the implementation of the protocol, i.e., the fact that the entanglement, between Alice and Bob, is never perfect and the fact that states teleported by Alice are near the vacuum state. After this analysis we performed an extension of the teleportation protocol by proposing a multi-channel protocol and studied the case of two channels in parallel. Finally, we created the first quantum cryptography protocol that uses the continuous variables teleportation protocol in an active way. We showed that this protocol is robust to the beam splitter attack and that this protocol is the only one working with direct reconciliation and without post-selection over the 50% loss scenario.

Sumário

Lista de Figuras

Lista de Tabelas

Lista de Abreviaturas

DCQVC	Distribuição de Chave Quântica em Variáveis Contínuas
DF	Divisor de Feixe
NEDT	Nenhum Estado é Deixado para Trás
PTVC	Protocolo de Teletransporte em Variáveis Contínuas
PTVCCP	Protocolo de Teletransporte em Variáveis Contínuas com Canais Paralelos

Capítulo 1

Introdução

A capacidade de comunicação de uma espécie é um fator determinante na sua evolução (Halliday, 1983, pg.166). Nenhuma espécie conhecida demonstra essa capacidade como a humana, a qual desenvolveu seu método de comunicação criando uma linguagem[1] (Atkinson, 2011; Houston, 2004) complexa representada por caracteres. Essa capacidade permitiu que mensagens fossem transmitidas por maiores distâncias tanto no tempo quanto no espaço. Graças à essa habilidade de se comunicar de forma eficiente podemos saber, por exemplo, o que egípcios pensavam há milhares de anos.

Ao analisarmos essa nossa dádiva evolutiva, vemos que ao nos expressarmos pela palavra, via comunicação oral, o ar flui através dos pulmões passando pelas cordas vocais que vibram. Essas vibrações provocam ondas de pressão longitudinais no ar que atingem os tímpanos, os quais vibram juntamente com um conjunto de ossos (martelo, bigorna, estribo e cóclea), transmitindo o sinal ao cérebro através do nervo acústico. Ao nos comunicarmos pela escrita, a fricção de dois materiais causa desgastes em um deles (ou em ambos), e esses desgastes são moldados em forma de caracteres definidos pela linguagem (escrita em pedra). Ou há deposito de um material sobre o outro (escrita com tinta) de tal maneira que haja um contraste que defina os caracteres. Analisando a nossa capacidade de comunicação por esse prisma, ao nos comunicarmos codificamos a mensagem em um ente físico para poder transmiti-la. Todo esse processo é regido por leis físicas (nos casos acima pelas leis da termodinâmica e as leis de Newton) e nesse sentido podemos afirmar que a *informação é física*.

Dessa maneira, vemos que a revolução na comunicação humana causada pela escrita deu-se devido à uma mudança de paradigma, ocasionada pela mudança do ente físico usado para transmitir a mensagem. Tal mudança permitiu que mensagens atravessassem eras, o que seria impossível utilizando-se a comunicação oral. Todavia, uma revolução maior em nossa comunicação ocorreu com os inventos do telégrafo sem fio em 1837 e do rádio em 1896. Com esses inventos mudamos o ente físico (e consequentemente as

[1] O vocábulo linguagem é entendido aqui como: *expressão do pensamento pela palavra, pela escrita ou por meio de sinais.*

leis físicas, sendo o ente físico agora regido pelas equações de Maxwell) no qual codificamos a informação. Ao codificarmos a informação em ondas eletromagnéticas passamos a nos comunicar à velocidade da luz e por maiores distâncias.

Estes exemplos ilustram o fato de que a mudança do ente físico usado para codificar a informação gera um aumento substancial na capacidade de comunicação. Embora haja mudança no ente físico (e nas leis da física que descrevem esse ente) usado para transmitir a informação, podemos dividir o processo de comunicação em certas partes essenciais (Reza, 2012, pg.4), como mostrado na Figura 1.1.

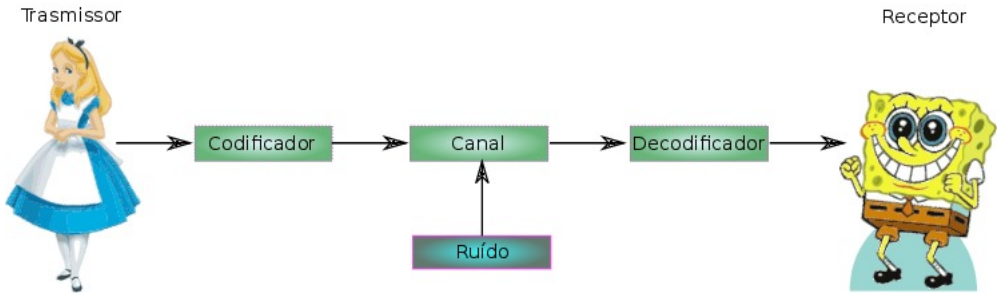


Figura 1.1: *Modelo do sistema de comunicação.*

Apresentamos na figura 1.1 uma representação esquemática das partes essenciais do processo de comunicação. Nela vemos que Alice (transmissor) codifica a mensagem e a envia através de um canal (ente físico), sendo essa mensagem descodificada e recebida por Bob (receptor). Note que há um processo chamado ruído que atua sobre o canal. Esse processo descreve a perda de informação pelo canal, a qual pode ser devido à ação do ambiente ou devido ao ataque de um espião que deseja saber o conteúdo da informação. Na comunicação oral, por exemplo, as ondas de pressão se propagam pelo ar carregando a informação e perdem energia para o ambiente a medida que se afastam da fonte (transmissor). Essa perda de energia é modelada como ruído atuando sobre o canal atenuando o sinal enviado.

Ao representarmos o processo de comunicação nesse modelo (Fig. 1.1), fica claro que o aumento na capacidade de comunicação da humanidade é devido à mudança do canal (e consequentemente a codificação e decodificação da informação nesse canal). Isso levanta uma importante questão, como quantificamos a informação que cada canal é capaz de suportar? Ou em outras palavras, como sabemos se um canal é melhor que outro? A resposta a essa pergunta foi dada por Claude Shannon (Shannon and Weaver, 1949) e por isso ele é conhecido como pai da teoria da informação.

1.1 Quantificação da informação

Para responder a essa pergunta Shannon teve que quantificar a informação e para isso ele tratou apenas da codificação da mensagem, desvencilhando esta de seu sig-

nificado. Em suas palavras "*...frequentemente, mensagens possuem significado; aspectos semânticos da comunicação são irrelevantes para o problema de engenharia. O aspecto significativo é que a mensagem real é uma seleção de um conjunto de mensagens possíveis*". Ao considerar a mensagem como uma seleção de um conjunto de mensagens possíveis, Shannon dá à informação um carácter probabilístico, definindo a informação por evento como:

$$I(E) = -\log_a(P(E)). \tag{1.1}$$

Onde a, a base, é uma constante positiva, E é o evento e $P(E)$ a probabilidade que esse evento ocorra. Note que quando $P(E) = 0$ a informação sobre esse evento é indeterminada ($I(E) = \infty$), o que é desejável pois indica a inviabilidade de obtenção de informação de um evento que não ocorra. A equação da informação (1.1) também tem a desejável propriedade de que, se o evento é certo ($P(E) = 1$), ele não traz nenhuma informação ($I(E) = 0$).

Utilizando as propriedades da função logarítmica podemos modificar a base da equação (1.1), $\log_a(P(E)) = (\log_a(b)) \log_b(P(E))$. Ao realizar essa mudança vemos que para $a > 0, b > 0, a \neq 1 \neq b$ e $P(E) > 0$ a função log difere de uma base para outra apenas por uma constante multiplicativa. Assim, ao usar a função logarítmica na quantificação da informação a mudança de base representa a mudança de unidade, ou seja, escolhendo a base escolhemos a unidade de informação (Hankerson et al., 2003, pg.27).

Shannon codifica a informação utilizando a álgebra binária definida por Boole (0 ou 1, verdadeiro ou falso, ligado ou desligado). Ao fazer isso Shannon escolhe usar a base 2 e defini a unidade de informação como *bit* (Shannon and Weaver, 1949), cujo nome é uma abreviação das palavras em inglês para dígito binário ("**bi**nary digi**t**"). Utilizando a codificação introduzida por Shannon há dois valores possíveis 0 e 1 para a informação. Logo a informação por caractere é dada por:

$$I(E = 1) = I(E = 0) = -\log_2\left(\frac{1}{2}\right) = 1\text{bit}. \tag{1.2}$$

A seleção entre dois eventos igualmente prováveis requer uma unidade de informação. Desse modo o *bit* é definido como a menor unidade de informação que pode ser processada, armazenada ou transmitida. Em outras palavras, o *bit* passa a ser a unidade básica de informação. Shannon consegue dessa forma quantificar a informação, de modo que todo pensamento humano pode ser expresso nessa nova base. A conversão da nossa linguagem para a binária, por exemplo, é feita através da tabela ASCII, a qual contém 255 caracteres entre letras, pontos e espaços. Se definirmos que esses caracteres são igualmente prováveis, necessitaremos de $I(E) = -\log_2(1/255) = 7.99bits$ ou 1 $bite$[2] para representar

[2] O *bite* é definido como um conjunto de 8 *bits*

cada caractere em linguagem binária. Shannon define também uma quantidade média de informação, a qual ele nomeia como entropia de informação (Reza, 2012, pg.79), definida por

$$H(X) = \overline{I(E_k)} = -\sum_{k=1}^{n} P(E_k)\log_2(P(E_k)), \tag{1.3}$$

onde a variável X é definida sobre o espaço de eventos $(E_1, ..., E_k)$. Pierce (2012) define entropia de informação como uma medida de incerteza de modo que quanto menor a incerteza (maior a probabilidade), menor a entropia e menor a quantidade de informação necessária. Dessa forma a entropia pode ser usada para quantificar os recursos necessários para armazenar informação, uma vez que ela quantifica a compressão ótima que pode ser alcançada sem que haja perda irreparável de dados (Nielsen and Chuang, 2004, pg.542).

Vejamos um exemplo. Ao realizarmos o cálculo da quantidade necessária de *bits* para a codificação binária da tabela ASCII na página anterior, levamos em conta que todos os caracteres possuem a mesma probabilidade. No entanto, alguns caracteres são mais usados que outros. Se definirmos, por exemplo, que as vogais têm uma probabilidade de 5% de serem enviadas, enquanto as consoantes têm uma probabilidade de 2%, e supormos que os demais caracteres têm a mesma probabilidade (aproximadamente 0.01%), a quantidade necessária de bits para a codificação seria $H(X) = 4bits$. Note que se esses valores fossem corretos, cada caractere da tabela ASCII poderia ser codificado em $4bits$. No entanto, a comunicação feita através desses caracteres depende de fatores regionais e portanto a frequência de uso de cada caractere depende da língua usada. Devido a isso a tabela ASCII possui cerca de $4bits$ de redundância.

Shannon fez uso da entropia para definir uma quantidade muito útil, denominada informação mútua,

$$I(X,Y) = H(X) + H(Y) - H(X,Y) = \sum_{x,y} P(E_x, E_y)\log_2\left[\frac{P(E_x, E_y)}{P(E_x)P(E_y)}\right]. \tag{1.4}$$

Aqui, $H(X,Y)$ é a entropia conjunta definida como $H(X,Y) \equiv -\sum_{x,y} P(x,y)\log_2(P(x,y))$, que representa a incerteza sobre o par de variáveis aleatórias (X,Y) e $P(x,y)$ é a probabilidade conjunta de x e y. Note que quando os eventos são independentes $P(x,y) = P(x)P(y)$ e consequentemente a informação mútua é zero.

A informação mútua mede a informação que flui através do canal (Reza, 2012, pg.105), correlacionando o conjunto de variáveis enviadas, X, com o conjunto de variáveis recebidas, Y. Dessa forma, quando essas variáveis são independentes (não há correlação) a informação mútua é zero. Num certo sentido, a informação mútua é uma medida de correlação entre as variáveis.

Por meio dessa análise probabilística Shannon conseguiu quantificar a in-

formação e, com essa quantificação, definir a quantidade mínima de recursos necessários para armazenar essa informação e ainda verificar a existência de correlações entre a informação enviada e recebida. Usando a informação mútua, Shannon ainda definiu a capacidade máxima de transmissão de um canal $C = \max(I(X, Y))$ (Reza, 2012, pg.109). Por meio de uma boa medida para a capacidade de um canal, Shannon também conseguiu modelar como a presença de ruído afeta a capacidade de transmissão de informação do canal. Para isso Shannon considerou o ruído atuando na variável Y, a qual está associada ao sinal visto pelo receptor. A existência do ruído faz com que y mude para $y - n$, onde n depende do tipo de ruído. Assim, a capacidade do canal na presença do ruído é $C = \max(I(x, y - n))$. Em suma, Shannon conseguiu descrever todo o processo de comunicação, quantificando o conteúdo informacional de cada mensagem e prevendo quanta informação cada canal poderia suportar.

1.2 Quantificação da informação em mecânica quântica

Com o advento da mecânica quântica houve uma nova quebra de paradigma, pois passamos a codificar a informação em estados quânticos. Essa nova codificação exigiu a mudança da unidade básica de informação, a qual é renomeada como qubit e definida levando em conta a superposição dos estados $|0\rangle$ e $|1\rangle$, matematicamente descrita como $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ (Nielsen and Chuang, 2004, pg.43), onde $|\alpha|^2 + |\beta|^2 = 1$. Ao supor uma sobreposição de estados ($|0\rangle$ e $|1\rangle$), a unidade básica de informação já não pode mais ser descrita pela álgebra de Boole e para representa-lá passamos a usar rótulos de vetores no espaço de Hilbert. Devido a essa mudança, tornam-se necessárias algumas modificações na teoria da informação de Shannon. Uma dessas modificações deve ser feita na definição da entropia de Shannon. Para realizarmos uma espécie de generalização da entropia de Shannon para estados quânticos, devemos fazer uso da entropia de von Neumann, definida como (Nielsen and Chuang, 2004, pg.552)

$$S(\rho) \equiv -Tr(\rho \log_2 \rho) = -\sum_x \lambda_x \log_2 \lambda_x. \tag{1.5}$$

Aqui, ρ descreve o estado quântico (operador densidade), λ_x são os autovalores de ρ e como na entropia de Shannon defini-se $0 \log_2 0 \equiv 0$. Note que a forma funcional da entropia não se modifica, a modificação está no uso do estado ρ no lugar das probabilidades. Assim, se supormos que as probabilidades são iguais aos autovalores de ρ, teremos $H(\lambda_x) = S(\lambda_x)$. Um fato interessante ocorre para estados puros, para os quais a entropia é igual a zero (Nielsen and Chuang, 2004, pg.555). A interpretação de Shannon nos diz que o estado puro não fornece informação alguma, ou seja, o estado puro é o estado com o máximo de informação possível e sua medida não trará nenhuma nova informação. Assim como a entropia de Shannon, as grandezas como informação mútua e capacidade do canal possuem

suas versões quânticas ((Nielsen and Chuang, 2004, pg.556) e (Nielsen and Chuang, 2004, pg.597), respectivamente). No entanto, elas não serão necessárias para o desenvolvimento dessa Tese e omitiremos suas definições.

Ao usarmos estados quânticos para codificar a informação, modificamos o canal por meio do qual a informação é transmitida. Essa modificação produz uma nova leva de ferramentas e recursos para a comunicação. Um grande exemplo desse novo recurso é o emaranhamento (Rigolin, 2005, pg.5), que será detalhado no capítulo 2, sessão 2.3. Essa correlação puramente quântica foi usada por Bennett and Wiesner (1992), para construir o protocolo de codificação superdensa. Esse protocolo permite que se envie dois bits de informação clássica através de um canal quântico emaranhado manipulando apenas um ente físico. Tarefa esta impossível via um canal clássico, mesmo ideal. A transmissão de dois bits de informação em um canal clássico requer pelo menos a manipulação e transmissão de duas partículas ou entidades físicas, as quais são usadas para a codificação da informação transmitida.

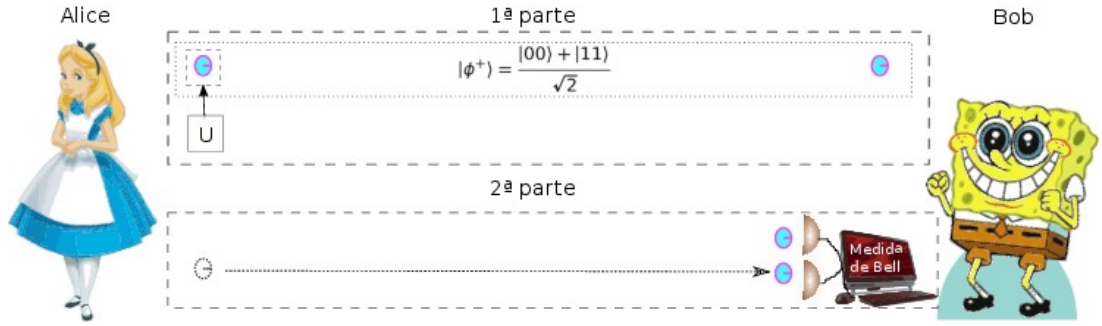


Figura 1.2: *Codificação superdensa.*

Para entendermos esse protocolo vamos imaginar que Alice e Bob inicialmente compartilham um estado maximamente emaranhado (veja figura 1.2). Note que o estado $|\phi^+\rangle$ foi previamente fixado, de modo que não há necessidade de Alice enviar qubits extras a Bob. Em vez disso, uma terceira pessoa pode previamente preparar o estado e mandar um qubit a Alice e o outro a Bob. Para uma melhor compreensão vamos dividir o protocolo em duas partes (figura 1.2). Na primeira parte Alice e Bob possuem um qubit cada. Alice deseja enviar dois bits de informação a Bob e para isso ela aplica uma operação unitária em seu qubit da seguinte maneira: caso Alice deseje enviar a sequência "00"de bits clássicos ela não fará nada com o seu qubit, ou seja, a transformação unitária aplicada será igual a identidade $U = \mathbb{1}_A$, $\mathbb{1}_A|\phi^+\rangle = |\phi^+\rangle$. Caso Alice deseje enviar a sequência de bits "01", a operação unitária deve ser então $U = \sigma_A^z$, de modo que $\sigma_A^z|\phi^+\rangle = |\phi^-\rangle$. Para enviar a sequência "10", Alice deverá realizar a operação unitária $U = \sigma_A^x$, com isso $\sigma_A^x|\phi^+\rangle = |\psi^+\rangle$. E finalmente, se Alice desejar enviar os bits "11", ela deve aplicar a operação $U = i\sigma_A^y$, de modo que $i\sigma_A^y|\phi^+\rangle = |\psi^-\rangle$. Aqui σ_k são as matrizes de Pauli, $\mathbb{1}$ é a matriz identidade e o subíndice A indica que o qubit está com Alice. Após aplicar a

Tabela 1.1: *Na primeira coluna (da esquerda para a direita), temos a codificação em bits que Alice deseja enviar, na segunda coluna as operações realizadas por Alice no seu qubit resultando nos estados da terceira coluna*

Bits	Operação aplicada por Alice	Resultado no estado
00	$\mathbb{1}_A\|\phi^+\rangle$	$\|\Phi^+\rangle = \frac{\|00\rangle+\|11\rangle}{\sqrt{2}}$
01	$\sigma_A^z\|\phi^+\rangle$	$\|\Phi^-\rangle = \frac{\|00\rangle-\|11\rangle}{\sqrt{2}}$
10	$\sigma_A^x\|\phi^+\rangle$	$\|\Psi^+\rangle = \frac{\|10\rangle+\|01\rangle}{\sqrt{2}}$
11	$i\sigma_A^y\|\phi^+\rangle$	$\|\Psi^-\rangle = \frac{\|10\rangle-\|01\rangle}{\sqrt{2}}$

operação unitária Alice encerra a primeira parte do protocolo, que pode ser sintetizado na tabela 1.1.

Alice inicia a segunda parte do protocolo enviando a Bob o seu qubit. Bob, em seguida, realizará uma medida de Bell nos dois qubits, descobrindo qual estado Alice enviou. Uma medida de Bell é aquela que permite diferenciar entre os quatro estados de Bell (última coluna da tabela 1.1). Dessa forma, utilizando a convenção da tabela 1.1, Bob lê a mensagem de dois bits enviada por Alice encerrando assim o protocolo. O uso do canal quântico, em particular o recurso de emaranhamento, permite que enviemos um número maior de informação transmitindo menos entes físicos de Alice para Bob.

1.3 Criptografia quântica

O uso de protocolos quânticos apresenta uma inovação que vai além do ganho na eficiência no envio de informação, sendo estendido inclusive a resoluções de problemas no âmbito da criptografia. A palavra criptografia vem do grego "*kryptós*", que significa escondido, e "*gráphein* ", que significa escrita, de modo que a criptografia é a ciência de cifrar informação para que apenas o transmissor e o receptor consigam entender. Ou seja, a criptografia é uma sub-área da comunicação que atua na codificação e na decodificação (ver figura 1.1) de uma mensagem, na expectativa de que apenas o transmissor e o receptor tenham acesso ao conteúdo da informação. Desse modo, a eficiência do código criptográfico está relacionada com o quão seguro ele é.

Atualmente o único código existente que possui um prova teórica sólida de segurança inquebrável (Shannon and Weaver, 1949) é conhecido como código de Vernam (Vernam, 1926) ou *one time pad*[3] (Rogers, 2010, pg.2). O código funciona de uma maneira relativamente simples. Supomos que Alice deseja enviar uma mensagem a Bob, que

[3]Em português esse código recebe o nome de chave de uso único.

é uma sequência de bits. Alice então cria uma "chave"consistindo de uma sequência completamente aleatória, exatamente do mesmo tamanho da sua mensagem (mesmo número de bits). Para encriptar a mensagem, Alice simplesmente realiza uma soma modular[4] de cada dígito da mensagem com o dígito correspondente da chave. Shannon provou que sob essas condições, absolutamente nenhuma informação está contida na mensagem codificada (Shannon and Weaver, 1949). Isso significa que, sem o conhecimento da chave de Alice não há como Bob extrair (decodificar) nenhuma parte da mensagem original a partir da transmissão criptografada (Rogers, 2010, pg.2).

Para garantir a segurança do código de Vernam, deve-se seguir algumas regras (Rogers, 2010, pg.2). A primeira é que a chave gerada por Alice deve ser verdadeiramente aleatória, porque qualquer correlação na chave pode ser usada por um "espião"para quebrar a mensagem codificada. Em segundo lugar, a chave deve ter exatamente o mesmo tamanho da mensagem e nunca deve ser reusada. Se alguma parte da chave for reutilizada, o espião pode examinar as mensagens codificadas somá-las e descobrir parte ou toda a chave. O problema com o código de Vernam é que a chave gerada por Alice precisa ser enviada a Bob, para que esse soma a chave da mensagem decodificando a mesma. E não há maneira (pelo menos clássica) de garantir o envio seguro da chave a Bob, já que informação clássica sempre pode ser copiada sem que alguém perceba.

O protocolo de encriptação de chave pública (também conhecido como protocolo de chaves assimétricas), como o RSA[5] ou o Diffie-Hellman, resolve o problema de distribuição de chave (Diffie and Hellman, 2006; Rivest et al., 1978). Esses protocolos utilizam problemas $NP-Completos$ (Nondeterministic Polynomial Time - Complete) para implementar algoritmos de criptografia. Esses algoritmos são baseados em problemas matemáticos que tem características úteis para a criptografia. Uma delas é o fato de que a obtenção da solução do problema é extremamente complicada, tempo computacional exponencial ou semi-exponencial, enquanto a verificação da solução é fácil. Dessa maneira, usa-se a solução para gerar a chave privada e o problema para gerar a chave pública. Como exemplo, podemos citar o protocolo RSA que utiliza a fatoração de números primos grandes. Resumidamente, Bob escolhe dois números primos grandes (por grandes quero dizer com centenas ou milhares de dígitos) p e q, tal que $N = pq$. Bob então usa p e q para calcular a chave privada. Para gerar a chave pública Bob usa N e um número inteiro escolhido por ele, e. Neste protocolo p e q são mantidos em sigilo enquanto o conhecimento de N e e é público.

É fácil obter N dado p e q. No entanto, para obter p e q dado N é um problema de fatoração cujo tempo de execução do melhor algoritmo existente (GNFS) torna o problema intratável para N grande (vide apêndice A). Dessa maneira, a segu-

[4]Soma aqui deve ser entendida como soma binária (ou soma módulo 2): $0+0=0$, $0+1=1$, $1+0=1$ e $1+1=0$.

[5]A descrição detalhada do protocolo está no apêndice A.

rança dos protocolos de chave pública reside na conjectura de que $NP \neq P$, ou seja, que não existe um algoritmo clássico que possa resolver problemas NP em tempo polinomial[6]. Embora não exista prova de sua segurança incondicional, protocolos baseados em problemas $NP-completos$ colocaram por terra qualquer tentativa de quebrá-los. Isso se manteve até 1994, quando Peter Shor demonstrou que um computador quântico (ou seja, que opere com qubits) poderia fatorar números primos grandes em um tempo polinomial (Shor, 1994). Dessa forma, o funcionamento do primeiro computador quântico atestaria o óbito de todo protocolo de criptografia que utiliza problemas $NP-completos$, já que esses problemas possuem a interessante propriedade de que ao encontrar uma solução eficiente para um problema, essa solução pode ser aplicada a todos os problemas $NP-completos$ (Rogers, 2010, pg.7).

O algoritmo de Shor (Shor, 1994) é um exemplo do poder da mudança de paradigma impulsionada pela mecânica quântica. Em tese, com ele podemos resolver problemas que classicamente não sabemos nem se há solução em tempo polinomial. Porém, ao resolver esses problemas o algoritmo de Shor demonstrou a fragilidade de nossos protocolos de criptografia (RSA, Diffie-Hellman e a criptografia de curva elíptica, entre outros) frente a essa nova codificação da informação dada pela mecânica quântica. No entanto, com a janela de oportunidade aberta por essa nova codificação, novos protocolos de criptografia foram criados (Bennett and Brassard, 1984; Bennett and Wiesner, 1992; Ekert, 1991) superando as falhas de seus antecessores clássicos.

Dentre esses protocolos, o de maior destaque, não só por ser o primeiro protocolo de criptografia quântica mas também pelo seu uso comercial (Van Assche, 2006, pg.159), é chamado BB84 (Bennett and Brassard, 1984). Esse protocolo, inventado por **B**ennett e **B**rassard em 1984, por isso o nome BB84, requer quatro estados e dois alfabetos binários: $|0\rangle$ e $|1\rangle$ (o alfabeto z), $|+\rangle \equiv |0\rangle_x = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$, $|-\rangle \equiv |1\rangle_x = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$ (o alfabeto x) (Benenti et al., 2004, pg.199). As "letras"dos alfabetos z e x estão associadas com os autoestados das matrizes de Pauli σ_z e σ_x, respectivamente.

Definido o alfabeto, Alice gera uma sequência aleatória de 0's e 1's codificando cada bit em um qubit, $|0\rangle$ ou $|0\rangle_x$ se o bit correspondente for 0 e $|1\rangle$ ou $|1\rangle_x$ caso o bit seja 1. Para cada bit, Alice escolhe aleatoriamente entre o alfabeto x ou z. Essa escolha pode ser feita através de uma moeda. Por exemplo, caso a moeda dê cara Alice escolhe o alfabeto x, se der coroa Alice então escolhe o alfabeto z. Alice envia essa sequência de qubits a Bob. Para cada qubit recebido Bob escolhe aleatoriamente qual eixo (alfabeto) será utilizado na medida, x ou z. No primeiro caso ele mede a polarização de spin ao longo

[6] Note que não existe uma demonstração de que isso seja verdade, sendo essa conjectura um dos problemas do milênio ainda em aberto propostos pelo instituto de matemática Clay, que considerou sete problemas matemáticos como os problemas do milênio. Quem resolver um desses problemas ganhará um prêmio de um milhão de dólares. Um desses problemas já foi resolvido, restando seis problemas ainda em aberto. A descrição dos problemas pode ser encontrada em "http://www.claymath.org/millennium-problems".

Tabela 1.2: *Exemplo do protocolo BB84*

Bits de Alice	1	0	0	0	1	1	0	1	0	1
Alfabeto de Alice	x	z	x	z	x	x	x	z	z	x
Qubtis transmitidos	$\|1\rangle_x$	$\|0\rangle$	$\|0\rangle_x$	$\|0\rangle$	$\|1\rangle_x$	$\|1\rangle_x$	$\|0\rangle_x$	$\|1\rangle$	$\|0\rangle$	$\|1\rangle_x$
Alfabeto de Bob	x	z	x	x	z	x	z	x	z	z
Resultado da medida	1	0	0	0	0	1	0	0	0	1
Bits de Bob	1	0	0	0	0	1	0	0	0	1
Raw key	1	0	0			1			0	1

do eixo x, e na segunda ao longo do eixo z. Note que metade das vezes Bob escolhe o mesmo eixo que Alice. Quando isso ocorre Alice e Bob compartilham o mesmo bit. Caso Bob escolha um eixo diferente de Alice, o bit resultante da medida de Bob concordará com o bit enviado por Alice apenas metade das vezes. Por exemplo, caso Bob receba o qubit $|1\rangle_x$ e realize a medida no eixo z, o resultado será 0 ou 1 com igual probabilidade.

Após as medidas Bob comunica a Alice, através de um canal público clássico, qual alfabeto ele usou para medir cada qubit. Bob comunica apenas o alfabeto (base) usado, nunca o resultado das medidas. Alice, por sua vez, comunica a Bob, através de um canal público clássico, o alfabeto (base) que ela utilizou para transmitir cada qubit. Depois de conferirem os resultados, Bob e Alice descartam todos os bits correspondentes aos casos em que usaram alfabetos diferentes. Após essa etapa eles compartilham a chamada *raw key* (em uma tradução literal, chave crua ou chave bruta) (Benenti et al., 2004, pg.200). Através de um canal de comunicação público, Alice e Bob anunciam e comparam parte da *raw key*. Dessa comparação eles podem estimar a *taxa de erro* (Kollmitzer and Pivk, 2010, pg.31) devido à espionagem ou efeitos de ruído. Se essa taxa for muito alta eles reiniciam o protocolo. Se não, eles aplicam protocolos de correção de erros como a *reconciliação de informação* e *amplificação de privacidade* nos restantes dos bits (Nielsen and Chuang, 2004, pg.628), obtendo assim uma chave segura. A tabela 1.2 mostra as escolhas de Bob e Alice e a geração da chave no protocolo BB84.

O protocolo BB84 utiliza propriedades da mecânica quântica para garantir o pleno funcionamento do protocolo *one time pad*. Ao utilizar dois alfabetos associados a dois observáveis que não comutam, σ_x e σ_z, o protocolo BB84 faz uso do princípio de incerteza de Heisenberg de maneira que Eva (a espiã) não poderá medir o qubit ao longo de x e z. Por exemplo, se Eva medir em σ_z o qubit $|0\rangle_x$, ela obterá como resultado 0 ou 1 com igual probabilidade. Assim, ela obterá um resultado aleatório para a polarização originalmente enviada por Alice. Além disso, caso Eva tente medir o qubit introduzirá erro no canal (devido ao postulado da medida, ver capítulo 2 seção 2.1) que será detectado quando Alice e Bob calcularem a taxa de erro. Como os qubits escolhidos para a codificação não são ortogonais, o teorema da não clonagem (veja capítulo 2 seção 2.2) garante que Eva não pode copiar os estados enviados por Alice. Com a prova teórica dada por Shannon de segurança do *one time pad*, e a garantia dada pela mecânica quântica de que as escolhas

dos bits são verdadeiramente aleatórias, o protocolo BB84 se tornou o primeiro protocolo teoricamente seguro. Após o BB84, vários outros protocolos de distribuição de chaves que utilizam propriedades quânticas surgiram (Ekert, 1991; Lo et al., 2005; Scarani et al., 2004).

1.4 Teletransporte quântico

Como acabamos de ver, a codificação da informação em sistemas quânticos nos dá um maior poder na transmissão de informação (Bennett and Wiesner, 1992), bem como uma maior segurança em sua transmissão (Ekert, 1991; Lo et al., 2005; Scarani et al., 2004). Mas além de fornecer uma maior eficiência em relação aos protocolos clássicos, a codificação da informação em sistemas quânticos possibilita a construção de um protocolo quântico que não possui nenhum antecessor clássico com o qual possa ser comparado. E de tão revolucionário este protocolo recebeu seu nome da ficção científica, o teletransporte quântico (Bennett et al., 1993). Este protocolo, embora não possa (ainda) teletransportar Spock até a Enterprise, pode enviar informação de um estado quântico desconhecido de um lugar a outro sem a necessidade de um ente físico para "transportar" essa informação. Devido a essa característica, Furusawa et al. (1998) define o teletransporte quântico como o transporte "desencarnado" de um estado desconhecido de um lugar a outro. O responsável por essa ação "fantasmagórica" é o emaranhamento (ver capítulo 2 seção 2.3), a mesma correlação responsável pela codificação super densa.

Resumidamente[7], o protocolo de teletransporte quântico funciona da seguinte maneira: Alice e Bob compartilham um estado maximamente emaranhado $|\Psi^-\rangle = \left(1/\sqrt{2}\right)(|01\rangle - |10\rangle))$ e um canal clássico de comunicação. Alice recebe um estado $\alpha|0\rangle + \beta|1\rangle$ desconhecido, o qual deseja "enviar"a Bob. Para enviar esse estado Alice procede como segue. Primeiramente ela realiza uma medida conjunta em seus estados (no qubit desconhecido e na sua parte do estado maximamente emaranhado) na base de Bell. Isso resulta em dois bits de informação, isto é, o resultado de sua medida. Alice então envia esse resultado a Bob através de um canal clássico. De posse desses dois bits de informação, Bob sabe qual correção deve fazer em seu estado para completar o teletransporte do estado desconhecido. Caso Bob receba os bits 00 ele não fará nada com seu estado, o que equivale a aplicação do operador identidade. Caso receba 10, Bob aplicará a operação σ_z em seu estado para completar o protocolo. Se ele receber 01, aplicará σ_x e finalmente se receber 11, ele aplicará as operações $\sigma_z\sigma_x$. Após a operação realizada por Bob o estado desconhecido outrora com Alice foi teletransportado a Bob.

Note que Alice desconhece o estado e portanto não pode dar nenhuma informação sobre ele a Bob através do canal clássico. É importante também salientar que

[7]Esse protocolo será explicado aqui de maneira resumida. Mas detalhes serão dados no capítulo 2, seção 2.4.

apesar de Alice e Bob compartilharem um estado quântico de duas partículas emaranhadas, essas estão espacialmente separadas não existindo nenhuma conexão entre elas a não ser a correlação quântica. O que torna esse protocolo realmente magnífico, é que ao final do protocolo o estado de Alice passa a ser descrito por um mistura estatística máxima. Isso indica que não houve cópia do estado, mas sim que toda a informação do estado outrora com Alice é transportada a Bob usando apenas dois bits de informação clássica e uma correlação puramente quântica.

Conforme vimos, a mudança de paradigma introduzida pela mecânica quântica produziu uma nova geração de protocolos de comunicação. No entanto, uma outra mudança de paradigma ocorreu tendo a própria mecânica quântica como protagonista. Essa mudança tem como pano de fundo os sistemas quânticos descritos por um espaço de Hilbert de dimensão infinita, como por exemplo modos do campo eletromagnético (Pirandola and Mancini, 2006), modos vibracionais de sólidos e condensados de Bose-Einstein (Weedbrook et al., 2012). Graças à dimensão infinita desse espaço de Hilbert, esses sistemas podem ser descritos por observáveis como posição e momento, que possuem um espectro contínuo de autovalores. Devido a esse tipo de espectro, esses sistemas são chamados de sistemas de variáveis contínuas (Pirandola and Mancini, 2006).

Conceitualmente esse novo paradigma pode ser visto como uma extensão dos estudos de protocolos de comunicação quântica de variáveis discretas para o de variáveis contínuas e, portanto, da dimensão finita para a infinita. No entanto, a principal motivação para o uso de variáveis contínuas em comunicação quântica teve uma origem mais prática (Braunstein and van Loock, 2005). Ao utilizarmos a óptica quântica para descrever campos eletromagnéticos quantizados em termos das suas quadraturas, é possível obter uma implementação eficiente dos passos essenciais dos protocolos de comunicação quântica. Ou seja, podemos preparar, manipular e medir estados quânticos de maneira eficiente (Braunstein and van Loock, 2005). Exemplos disso são as medidas nas quadraturas que possuem eficiência próxima a 100% e deslocamentos do modo óptico no espaço de fase, por meio das técnicas de detecção homódina e feedforward (Braunstein and van Loock, 2005).

Outra vantagem no uso de estados de variáveis contínuas reside no fato da produção eficiente de estados emaranhados a partir de estados comprimidos e óptica linear (Braunstein and van Loock, 2005). Porém, essa efetividade na produção de estados emaranhados tem o seu preço, e esse preço é a imperfeição dos estados emaranhados. O grau de imperfeição dependerá da quantidade de compressão do estado. Em outras palavras, utilizando-se das técnicas desenvolvidas no âmbito da óptica quântica, a implementação de protocolos de comunicação quântica via variáveis contínuas sempre dá um sinal de saída ("funciona"). Contudo, nem sempre obtemos um sinal limpo e perfeito. Já no caso dos protocolos de comunicação baseados em variáveis discretas, sua implementação às vezes não produz um sinal de saída ("não funciona"). Mas quando funciona temos uma

execução quase perfeita. Um exemplo dessa distinção, aparece ao enviarmos um estado através de um canal com ruído, fibras ópticas por exemplo. Devido a perdas o estado de variáveis contínuas acumula ruído e emerge para o receptor como uma versão contaminada do estado de entrada. O estado de variáveis discretas, como por exemplo a polarização de um único fóton, dependendo do ruído pode ser absorvido e nenhuma informação emergirá para o receptor (Braunstein and van Loock, 2005).

Aproveitando a vantagem prática dada pelos sistemas ópticos de variáveis contínuas, os protocolos como a codificação superdensa (Ban, 1999), criptografia quântica (Grosshans and Grangier, 2002; Grosshans et al., 2003; Ralph, 1999) e o teletransporte quântico (Braunstein and Kimble, 1998; Vaidman, 1994) foram descritos em termos de variáveis contínuas. Nesta Tese nosso foco será estudar o protocolo de teletransporte quântico em variáveis contínuas (PTVC). A extensão do protocolo de variáveis discretas a variáveis contínuas foi feita inicialmente por Vaidman (1994) para estados não-físicos e em seguida feita em termos das quadraturas do campo eletromagnético por Braunstein and Kimble (1998) para estados físicos (compressão finita). Na descrição feita por Braunstein and Kimble (1998), Alice e Bob compartilham um estado comprimido de dois modos (esse estado está emaranhado e seu emaranhamento é proporcional a compressão desses modos). Alice então recebe um estado coerente desconhecido $|\alpha\rangle$ (descrito em termos de suas quadraturas) que deseja enviar a Bob. Alice interage esse estado desconhecido com o seu modo do canal (estado comprimido) através de um divisor de feixes (DF) e em seguida realiza medidas homódinas em seus estados obtendo a posição de um estado e o momento de outro. De posse do resultado dessas medidas, Alice as envia a Bob através de um canal clássico, que por sua vez as usa para realizar os deslocamentos nas quadraturas do seu estado, encerrando o protocolo de teletransporte.

Ao compararmos o PTVC com o protocolo de teletransporte discreto, podemos perceber que a diferença entre ambos reside no tipo de interação entre as entidades físicas (e obviamente a dimensão do espaço de Hilbert). Enquanto no protocolo discreto essa interação é dada pela medida de Bell realizada por Alice, no PTVC a interação de Alice é realizada pela operação do divisor de feixes juntamente com a medida homódina. A interação de Bob continua a depender das medidas realizadas por Alice, mudando apenas o operador unitário que ele utiliza (deslocamentos na quadraturas para PTVC e matrizes de Pauli para o protocolo discreto). Assim como no protocolo discreto, no PTVC o estado só é perfeitamente teletransportado quando o canal é maximamente emaranhado. No entanto, como havíamos mencionado anteriormente, em variáveis contínuas o emaranhamento depende da compressão do estado, e um estado maximamente emaranhado exigiria uma compressão infinita, o que descreveria um estado que não possui existência física. Portanto, realizar um PTVC perfeito é impossível. Todavia, com o avanço tecnológico estados com um maior parâmetro de compressão, r, são atingidos. Hoje, o estado da arte na compressão de estados produz estados com fator de compressão $r \approx 10dB$ (Eberle

et al., 2013).

Dada a impossibilidade de se teletransportar um estado em variáveis contínuas perfeitamente, usando um estado comprimido físico (compressão r finita), tomamos como objetivo central desta Tese estudar o PTVC com o intuito de modificá-lo para criar protocolos de comunicação que funcionem perfeitamente ou sejam mais eficientes utilizando-se emaranhamento finito (baixo parâmetro de compressão). O estudo detalhado do PTVC nos permitirá conhecer as limitações de cada etapa do protocolo para, em seguida, realizar modificações nestas etapas a fim de obter um novo protocolo mais eficiente. Além disso, queremos adicionar novos elementos ao PTVC original de maneira a criar uma nova possibilidade de teletransporte. Podemos ainda usar esse conhecimento em outra área da comunicação quântica, criando um protocolo de criptografia quântica que tenha o PTVC como recurso fundamental em sua construção.

Para alcançar nossos objetivos, inicialmente realizamos uma revisão no capítulo 2 dos postulados da mecânica quântica. Apresentamos também as consequências destes postulados mais relevantes para os assuntos estudados nesta Tese. Uma dessas consequências é o teorema da não clonagem (Wootters and Zurek, 1982), o qual afirma a impossibilidade de copiar estados quânticos não ortogonais arbitrários. Este teorema é um dos fatores que garante a segurança na criptografia quântica. Em sequência revisamos outra consequência dos postulados da mecânica quântica, o emaranhamento (Rigolin, 2005, pg.5). Essa fantástica correlação quântica surge naturalmente ao aplicarmos o princípio da superposição em sistemas quânticos compostos, revelando o aspecto não-local da mecânica quântica. O emaranhamento, conforme veremos, possui um papel fundamental nos protocolos de teletransporte em variáveis discretas e contínuas. Prosseguindo com nossa revisão, descrevemos de forma detalhada o protocolo de teletransporte em variáveis discretas (Bennett and Wiesner, 1992), de modo a identificar o papel fundamental do emaranhamento em sua operação. Em seguida definimos um método para mensurar a eficiência do protocolo de teletransporte, chamado de fidelidade. Por fim, encerramos nossa revisão introduzindo por meio da óptica quântica o formalismo matemático associado às variáveis contínuas. Neste capítulo também apresentamos o formalismo relacionado às quadraturas dos modos do campo eletromagnéticos, os estados que serão utilizados nos protocolos e as operações quânticas necessárias para se implementar os protocolos desta Tese.

No capítulo 3 descrevemos o PTVC na representação de Schrödinger, utilizando operações quânticas mais gerais do que originalmente usadas por Braunstein and Kimble (1998). Procedendo desta forma alcançamos o primeiro resultado original desta Tese. Mostramos que estas operações quânticas mais gerais podem ser otimizadas para aumentar consideravelmente a eficiência do PTVC, mesmo quando Alice e Bob compartilham um canal fracamente emaranhado. O ponto chave neste ganho de eficiência reside no fato de que na prática Alice e Bob sempre têm um conhecimento prévio sobre os possíveis estados a serem teletransportados Luiz and Rigolin (2013).

No capítulo 4, desenvolvemos um novo PTVC multicanais, composto por n canais, dispostos de forma paralela. Esse protocolo surge como uma adaptação do protocolo de teletransporte híbrido de Andersen and Ralph (2013). Assim como o protocolo de Andersen and Ralph (2013), nosso protocolo tem o intuito de dividir o estado a ser teletransportado em várias partes através de divisores de feixe para, em seguida, teletransportar essas partes através de canais distintos. Para verificar a eficiência de nosso protocolo realizamos um estudo inicial com dois canais. Nessa configuração mostramos que igualamos a eficiência do PTVC original (Braunstein and Kimble, 1998) e superamos a eficiência dos protocolos de Andersen and Ralph (2013) e Furusawa et al. (1998).

No capítulo 5 apresentamos outro resultado original (Luiz and Rigolin, 2014), qual seja, um protocolo de distribuição de chaves quântico (DCQ). Esse protocolo é baseado no PTVC de estados coerentes, gerando uma chave secreta bruta (raw key) constituída de variáveis discretas, tanto para Alice e Bob. Ou seja, apesar de usarmos variáveis contínuas este protocolo possui uma codificação discreta para a chave, fato este que aumenta sua eficiência. De fato, com este protocolo preservamos os esquemas de detecção eficientes das variáveis contínuas e, ao mesmo tempo, usamos algoritmos de correção de erro e de amplificação de privacidade eficientes para uma codificação binária da chave. Devido a isso, nosso protocolo é seguro para perdas superiores a 90% no canal óptico utilizado por Alice para transmitir a Bob o seu modo emaranhado. Além disso, nosso protocolo de distribuição de chaves quântico em variáveis contínuas (DCQVC) funciona de forma determinística (sem a necessidade de se realizar pós-seleção) e faz uso de algoritmos de correção de erros conhecidos por reconciliação direta. Na análise de segurança do protocolo, realizamos o ataque incoerente chamado ataque de divisor de feixes. Nesse ataque, Eva rouba parte do sinal de Bob e tenta realizar operações na parte roubada do sinal de modo a obter a chave. Nesse contexto, mostramos que nosso protocolo é seguro até com uma perda de sinal próxima a 100%, ou seja, mesmo que Eva roube quase todo sinal o protocolo ainda permanece seguro. Este é o único protocolo com reconciliação direta a operar nesse regime de tão altas perdas.

Finalmente, no capítulo 6 expomos nossas conclusões sobre os assuntos aqui estudados, relembrando os pontos mais relevantes e sugerindo possíveis desdobramentos decorrentes dos protocolos aqui apresentados.

Capítulo 2

Conceitos teóricos básicos

A teoria da informação quântica é um campo de pesquisa interdisciplinar, sendo composto fundamentalmente pela mecânica quântica e a teoria da informação. Mas não podemos esquecer o que disse Rolf Landauer, *"A informação é física"*. Queremos dizer com isso que toda informação é processada, armazenada ou transmitida utilizando um meio (sistema físico) que obrigatoriamente obedece às leis da física. A teoria da informação quântica, em particular a subárea da teoria da comunicação quântica, deve obedecer aos postulados da mecânica quântica. Tendo isso em vista, nesse capítulo faremos uma breve introdução a estes postulados levando à luz da interpretação de Copenhagen. A teoria da informação quântica pode ser estudada por meio de vários sistemas físicos diferentes (Lee et al., 2011; Olmschenk et al., 2009; Pfaff et al., 2014). Aqui escolhermos utilizar os sistemas ópticos. A escolha desse sistema leva em conta a sua aplicabilidade experimental em protocolos de variáveis contínuas (Furusawa et al., 1998; Lee et al., 2011). Devido à escolha desse sistema, neste capítulo, juntamente com os postulados da mecânica quântica, faremos uma breve introdução à óptica quântica.

2.1 Postulados da mecânica quântica

Toda teoria física contém conceitos físicos, formalismo matemático e um conjunto de regras de correspondência que mapeiam os conceitos físicos aos objetos matemáticos que os representam (Ballentine, 1998, pg.42). Logo, para obter um arcabouço conceitual de modo a compreender os fenômenos da natureza, torna-se necessário elaborar conceitos físicos (por exemplo, momento, força, etc...), utilizar uma linguagem de estrutura lógica bem definida (formalismo matemático) e um conjunto de regras, as quais associam os conceitos físicos a essa linguagem.

Esse arcabouço conceitual é dado na mecânica quântica por seus postulados e para um melhor entendimento desses postulados é necessário realizar algumas definições prévias. A primeira definição diz respeito ao sistema físico estudado. Adotaremos a definição usada na referência Galindo et al. (2012) pg.34, a qual define o sistema físico como

sendo uma pequena parte do universo que está isolada para todos os efeitos práticos ou, pelo menos, que se tenha controle sobre as influências externas atuando sobre o sistema. Supomos, também, que este sistema seja suscetível à manipulação experimental. Após submeter o sistema a uma série apropriada de operações experimentais, este será deixado no que chamamos de um *estado* do sistema. Em particular, nós podemos dizer que quando o estado desse sistema é *puro* nosso conhecimento sobre o estado é o máximo possível. De posse dessas definições, estamos aptos a enunciar o primeiro postulado da mecânica quântica.

Postulado I *"A descrição de um sistema físico em mecânica quântica é realizada em termos dos elementos de um espaço de Hilbert complexo associado ao sistema físico. Em um dado instante de tempo t, um estado puro de um sistema físico é representado no espaço de Hilbert correspondente por um raio*[1] *unitário* $|\psi(t)\rangle_R$*. Um elemento* $|\psi(t)\rangle$ *do raio* $|\psi(t)\rangle_R$ *é chamado vetor de estado, ou ket."* (Galindo et al., 2012, pg.37)

O Postulado I é uma regra de correspondência que associa (ou mapeia) o estado de um sistema físico (conceito físico) à um raio no espaço de Hilbert (objeto matemático). Ao realizar essa associação, o Postulado I nos diz que a mecânica quântica é formulada em termos de um espaço vetorial complexo (espaço de Hilbert), geralmente de dimensão infinita[2], e munido de um produto escalar hermitiano (Toledo Piza, 2009, pg.47).

Como podemos ver acima, a notação do vetor de estado ou ket, chamada notação de Dirac, é indicada pelo símbolo $|\rangle$, e especificada pelo rótulo identificador como por exemplo, ϕ, ψ, ψ_1, etc. No espaço de Hilbert estão definidos as operações de soma de vetores[3] e de produto de um vetor por um número complexo z. A definição dessas operações é tal que a soma de dois vetores associa a dois vetores quaisquer, $|\phi\rangle$ e $|\psi\rangle$, um terceiro vetor $|\chi\rangle = |\phi\rangle + |\psi\rangle$[4]. Também devemos satisfazer as propriedades associativa, comutativa, a existência de um vetor nulo e do elemento inverso, $|\phi\rangle + |\tilde{\phi}\rangle = |\emptyset\rangle$. O produto de um vetor $|\phi\rangle$ por um número complexo z, tem como resultado um vetor $z|\phi\rangle$ e satisfaz as propriedades distributiva e associativa em relação a multiplicação. O produto de qualquer vetor por $z = 1$ reproduz o mesmo vetor, $1|\phi\rangle = |\phi\rangle$ para qualquer $|\phi\rangle$.

Uma classe importante de objetos que é possível definir em um espaço vetorial é a classe de todas as funções lineares com valores complexos cujo argumento é um vetor do espaço (Toledo Piza, 2009, pg.49), ou seja, o espaço adjunto. A notação introduzida por Dirac para esses objetos é $\langle|$, sendo chamada de bra. Funções lineares

[1] De uma maneira didática, e no mais simples dos casos, pode-se pensar o raio como uma extensão lógica do conceito de um vetor unitário que inclui fases arbitrárias, ou seja, um conjunto de vetores unitários que diferem entre si apenas por uma fase formam um raio

[2] A exata natureza do espaço de Hilbert depende do sistema considerado. Nesse trabalho iremos considerar sistemas descritos no espaço de Hilbert das funções de Lebesgue quadrado integrável L^2.

[3] A partir daqui usaremos vetor com significado de vetor de estado ou ket.

[4] Salientamos que nesse caso esse estado não esta normalizado. Devemos lembrar que o primeiro postulado afirma que esses raios são unitários, logo $|\chi\rangle$ também deve ser unitário.

específicas são designadas por rótulos identificadores como ϕ, ψ, etc. e aparecem sob a forma $\langle\phi|$, $\langle\psi|$, etc. De modo que o resultado da ação do bra $\langle\phi|$ sobre o ket $|\psi\rangle$ será um número complexo representado por $\langle\phi|\psi\rangle$. A linearidade dos bras significa que $\langle|(z_1|\phi\rangle + z_2|\psi\rangle) = z_1\langle|\phi\rangle + z_2\langle|\psi\rangle$, ou seja, o número complexo que resulta da aplicação de uma função linear qualquer a uma combinação linear de vetores, é a mesma combinação linear dos números complexos que resultam da aplicação dessa função a cada um dos dois vetores separadamente.

Sobre o conjunto das funções lineares define-se a soma (associativa e comutativa) de duas funções e o produto de uma função por um número complexo respectivamente através das relações (Toledo Piza, 2009, pg.49), $(\langle\chi| + \langle\psi|)|\phi\rangle = \langle\chi|\phi\rangle + \langle\psi|\phi\rangle$ e $(z\langle\chi|)|\phi\rangle = z\langle\chi|\phi\rangle$. Também é possível definir uma função nula $\langle\emptyset|$ através da relação $\langle\emptyset|\phi\rangle = 0$ válida para qualquer $|\phi\rangle$, e associar a cada função $\langle\chi|$ uma função $\langle\tilde{\chi}|$ através de $\langle\tilde{\chi}|\phi\rangle = -\langle\chi|\phi\rangle$. De modo que, $\langle\chi| + \langle\tilde{\chi}| = \langle\emptyset|$. Dessas definições resulta que o conjunto das funções lineares sobre o espaço vetorial tem uma estrutura de espaço vetorial. Este novo espaço vetorial é chamado de *espaço dual* do espaço de partida (Toledo Piza, 2009, pg.49).

Como dissemos anteriormente, o espaço de Hilbert é munido de um produto escalar e podemos representar essa operação associando a todo par de vetores $|\phi\rangle$ e $|\psi\rangle$ um número complexo através das funções lineares. Esta operação é indicada por $\langle\phi|\psi\rangle$. Dessa maneira, estabelecemos uma correspondência biunívoca entre os vetores do espaço de partida e os vetores do espaço dual através do produto escalar definido no espaço de partida. Essa correspondência é feita de maneira mais formal pelo teorema de Riesz (Ballentine, 1998, pg.10). Assim, para estabelecer essa correspondência basta associar a cada vetor $|\varphi\rangle$ a função linear a ser definida como $\langle\varphi|$, tal que o seu valor em qualquer vetor $|\psi\rangle$ seja igual ao produto escalar de $|\varphi\rangle$ e $|\psi\rangle$. As seguintes propriedades devem ser satisfeitas. O produto escalar de um vetor $|\varphi\rangle$ com a soma de dois outros $|\chi\rangle = |\psi_1\rangle + |\psi_2\rangle$ é igual à soma dos produtos escalares desse vetor com cada um dos vetores envolvidos na soma, $\langle\varphi|\chi\rangle = \langle\varphi|\psi_1\rangle + \langle\varphi|\psi_2\rangle$; $\langle\varphi|z\psi\rangle = z\langle\varphi|\psi\rangle$, sendo z um número complexo; $\langle\varphi|\psi\rangle = \langle\psi|\varphi\rangle^*$, onde o asterisco indica conjugação complexa; e para todo vetor $|\varphi\rangle$, $0 \leq \langle\varphi|\varphi\rangle < \infty$, sendo que a igualdade a zero se dá se, e somente se, $|\varphi\rangle = |\emptyset\rangle$.

A segunda e terceira propriedades implicam que $\langle z\varphi|\psi\rangle = z^*\langle\varphi|\psi\rangle$. Juntamente com a primeira propriedade elas implicam na linearidade do produto escalar com relação ao ket e no que se chama anti-linearidade com relação ao bra, que pode ser escrito respectivamente, $\langle\varphi|z_1\psi_1 + z_2\psi_2\rangle = z_1\langle\varphi|\psi_1\rangle + z_2\langle\varphi|\psi_2\rangle$ e $\langle z_1\psi_1 + z_2\psi_2|\varphi\rangle = z_1^*\langle\psi_1|\varphi\rangle + z_2^*\langle\psi_2|\varphi\rangle$. Uma consequência importante da definição do produto escalar é conhecida como desigualdade de Schwarz. Ela afirma que, para quaisquer dois vetores, $|\varphi\rangle$ e $|\psi\rangle$, vale a relação[5]

$$|\langle\varphi|\psi\rangle|^2 \leq \langle\varphi|\varphi\rangle\langle\psi|\psi\rangle. \tag{2.1}$$

[5]Ver a demostração no apêndice B.

A existência do produto escalar permite definir uma norma para os vetores do espaço de Hilbert como $\|\varphi\| = \langle\varphi|\varphi\rangle^{1/2}$, que deve satisfazer as seguintes propriedades: $0 \leq \|\varphi\| \leq \infty$ para qualquer vetor $|\varphi\rangle$, sendo igual a zero se, e somente se, $|\varphi\rangle = |\emptyset\rangle$; $\|\varphi+\psi\| \leq \|\varphi\|+\|\psi\|$ para quaisquer $|\varphi\rangle$,$|\psi\rangle$; $\|z\varphi\| = |z|\|\varphi\|$, onde z é um número complexo e $|z|$ é o seu módulo, para qualquer $|\varphi\rangle$. O produto escalar implementa a ideia "geométrica" de ortogonalidade de dois vetores através do anulamento de seu produto escalar, $\langle\phi_i|\phi_j\rangle = \delta_{ij}$, onde δ_{ij} é o delta de Kronecker. O espaço de Hilbert ainda é dotado de uma propriedade chamada *completeza*.

Se o conjunto de vetores $\{x\}$ é *completo*, ou seja, forma uma base que abrange o espaço vetorial, então podemos expandir qualquer vetor arbitrário $|\phi\rangle$ em termos desse conjunto, $|\phi\rangle = \int_{-\infty}^{+\infty} dx\phi\,(x)\,|x\rangle$. Aplicando o bra $\langle x'|$ temos $\langle x'|\phi\rangle = \int_{-\infty}^{+\infty} dx\phi\,(x)$ $\delta\,(x - x')$ de modo que $\phi\,(x') = \langle x'|\phi\rangle$. Como x' é uma variável arbitrária podemos escrever o estado como

$$|\phi\rangle = \int_{-\infty}^{+\infty} dx|x\rangle\,(\langle x|\phi\rangle) = \left(\int_{-\infty}^{+\infty} dx|x\rangle\langle x|\right)|\phi\rangle. \tag{2.2}$$

Os parênteses são desnecessários e usados apenas para enfatizar as duas interpretações da equação (2.2). A primeira sugere que o vetor $|\phi\rangle$ é igual a integração dos vetores da base multiplicada por um coeficiente escalar. A segunda sugere que algo atuando no estado, o que chamaremos de operador, resulta no próprio vetor. Logo, para qualquer vetor $|\phi\rangle$, este operador deve ser o operador identidade,

$$\mathbb{1} = \int_{-\infty}^{+\infty} dx|x\rangle\langle x|. \tag{2.3}$$

Antes de prosseguirmos devemos esclarecer alguns pontos. Para chegarmos ao operador identidade supomos que $\langle x'|x\rangle = \delta\,(x - x')$. Essa definição foi proposta por Dirac no formalismo da mecânica quântica e por isso a "função" $\delta\,(x - x')$ leva o seu nome. Essa função, ou melhor, distribuição, possui uma peculiaridade quando $x' = x$. Neste ponto ela torna-se infinita. Pela definição da norma isso daria uma norma infinita e portanto fora do espaço de Hilbert. Embora a função delta de Dirac seja divergente neste ponto, podemos representar o estado como uma distribuição de estados no que convencionamos chamar de base da posição, de modo que o produto escalar se torna finito $\int_{-\infty}^{+\infty} dx\phi\,(x)\,\delta\,(x - x') = \phi\,(x') < \infty$. É possível demonstrar que o conjunto de vetores $\{x\}$ é completo[6] no *rigged Hilbert space*[7], que nada mais é do que um espaço de Hilbert estendido. O espaço dual estendido contém a função delta de Dirac e as funções exponenciais complexas de modo

[6]O ferramental matemático exigido para tal demostração foge do escopo dessa Tese. Por esse motivo não realizaremos a demostração, que pode ser encontrada na página 106 da referência Gelfand and Vilenkin (1964).

[7]Segundo a referência (Ballentine, 1998), página 28, o termo "rigged" tem como interpretação "equipado e pronto para a ação". Já a referência (Griffiths, 2011), página 80, nomeia esse espaço como *espaço de Hilbert estriado.*

que o tratamento em dimensões infinitas se torna mais natural nesse espaço (Ballentine, 1998, pg.29).

Ao definimos o operador identidade, observamos que existe uma classe de objetos que atua sobre os elementos do espaço de Hilbert. Esses objetos são denominados operadores lineares e possuem uma importância vital para a mecânica quântica. Tal importância é expressa no seguinte postulado.

Postulado II. *"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 um tempo t_2 por um operador unitário $\hat{U}$ que depende somente de t_1 e t_2 "*(Nielsen and Chuang, 2004, pg.110)

$$|\psi'\rangle = \hat{U}|\psi\rangle. \tag{2.4}$$

Assim como o primeiro postulado, o segundo postulado oferece uma regra de correspondência, associando a evolução de um sistema físico a um ente matemático. Alguns pontos do segundo postulado merecem esclarecimentos, como por exemplo o que vem a ser um operador unitário. Porém, antes de fornecer esses esclarecimentos, é necessário destacar algumas propriedades dos operadores lineares. Um operador linear $\hat{A}$ atuando em um espaço de Hilbert transforma vetores desse espaço em outro vetor do mesmo espaço, $\hat{A}|\varphi\rangle = |\psi\rangle$. E a aplicação de operadores lineares em uma combinação linear de vetores é dada da forma, $\hat{A}\left(z_1|\varphi_1\rangle + z_2|\varphi_2\rangle\right) = z_1\hat{A}|\varphi_1\rangle + z_2\hat{A}|\varphi_2\rangle$. A soma e o produto de operadores lineares pode ser definida através das relações;$(\hat{A}+\hat{B})|\varphi\rangle = \hat{A}|\varphi\rangle + \hat{B}|\varphi\rangle$ e $(\hat{A}\hat{B})|\varphi\rangle = \hat{A}(\hat{B})|\varphi\rangle$, que também correspondem a operadores lineares. Em geral $\hat{A}(\hat{B}|\varphi\rangle) \neq \hat{B}(\hat{A}|\varphi\rangle)$, o que equivale a dizer que os operadores não comutam, $[\hat{A},\hat{B}] = \hat{A}\hat{B} - \hat{B}\hat{A} \neq 0$. O produto de um operador linear por um número complexo também é definindo simplesmente como $(z\hat{A})|\varphi\rangle = z(\hat{A}|\varphi\rangle)$.

É possível associar a cada operador $\hat{A}$ outro operador $\hat{A}^\dagger$ chamado operador adjunto de $\hat{A}$, através da relação $\langle\varphi|\hat{A}^\dagger|\psi\rangle = \langle\psi|\hat{A}|\varphi\rangle^*$, válida para quaisquer vetores $|\varphi\rangle$ e $|\psi\rangle$. O operador adjunto ainda tem as propriedades: $(\hat{A}^\dagger)^\dagger = \hat{A}$, já que $\langle\varphi|(\hat{A}^\dagger)^\dagger|\psi\rangle = \langle\psi|\hat{A}^\dagger|\varphi\rangle^* = \langle\varphi|\hat{A}|\psi\rangle$; $(\hat{A}+\hat{B})^\dagger = \hat{A}^\dagger + \hat{B}^\dagger$; $(\hat{A}\hat{B})^\dagger = \hat{B}^\dagger\hat{A}^\dagger$, pois $\langle\varphi|(\hat{A}\hat{B})^t|\psi\rangle = \langle\psi|\hat{A}\hat{B}|\varphi\rangle^* = \langle\varphi|\hat{B}^\dagger\hat{A}^\dagger|\psi\rangle$; $(z\hat{A})^\dagger = z^*\hat{A}^\dagger$, onde z é um número complexo.

Um operador $\hat{A}$ igual ao seu adjunto $\hat{A}^\dagger$ é chamado *operador auto adjunto*. Isto implica $\langle\varphi|\hat{A}|\psi\rangle = \langle\psi|\hat{A}|\varphi\rangle^*$ e que o domínio de $\hat{A}$ (ou seja, o conjunto de vetores $|\varphi\rangle$ em que $\hat{A}|\varphi\rangle$ é bem definido) coincide com o domínio de $\hat{A}^\dagger$. Um operador que somente satisfaz $\langle\varphi|\hat{A}^\dagger|\psi\rangle = \langle\psi|\hat{A}|\varphi\rangle^*$ é chamado de Hermitiano (Ballentine, 1998, pg.15). Se um operador atuando sobre um vetor produz um escalar vezes o mesmo vetor, $\hat{A}|\varphi\rangle = a|\varphi\rangle$, o vetor $|\varphi\rangle$ é então chamado de autovetor e o escalar a de autovalor do operador $\hat{A}$. A correspondência antilinear entre bras e kets e a definição de operador adjunto $\hat{A}^\dagger$

implicam na equação de autovalores para os bras, $\langle\varphi|\hat{A}^\dagger = a^*\langle\varphi|$. Com a equação de autovalor é fácil verificar que se o operador $\hat{A}$ é Hermitiano todos os autovalores são reais[8] e que autovetores que correspondem a autovalores distintos para um operador Hermitiano devem ser ortogonais[9].

Há duas classes de operadores lineares que possuem grande relevância na mecânica quântica. A primeira delas é descrita pelo segundo postulado, a classe dos *operadores unitários*, identificados pela propriedade $\hat{U}\hat{U}^\dagger = \hat{1}$. A ação de operadores unitários preserva o produto escalar (e portanto a norma). Em particular um operador unitário transforma uma base ortonormal em outra base ortonormal do espaço vetorial. Além disso o produto de operadores unitários é ainda um operador unitário. Esses operadores são usados para evoluir o sistema (ou seja, levar um estado para outro estado, como define o segundo postulado). Outro ponto destacado pelo segundo postulado é o fato de esses operadores evoluírem um sistema *fechado*. Por *fechado* queremos dizer um sistema idealmente isolado (livre de ação externa). Ao evoluir o estado em um sistema quântico fechado, essa evolução temporal é descrita pela equação de Schrödinger[10] o que leva o operador unitário a assumir a forma $e^{-i\hat{H}t/\hbar}$, sendo $\hat{H}$ um operador hermitiano conhecido como Hamiltoniano do sistema.

A segunda classe de operadores é chamada de *operadores de projeção*, e é identificada pelas propriedades $\hat{P}^\dagger = \hat{P}$ e $\hat{P}^2 \equiv \hat{P}\hat{P} = \hat{P}$. A primeira propriedade nos indica que os operadores de projeção são Hermitianos e a segunda propriedade é conhecida como *idempotência* (Toledo Piza, 2009, pg.56). Com o uso do operador de projeção podemos escrever qualquer vetor $|\varphi\rangle$ na base completa $|x\rangle$ como

$$|\varphi\rangle = \int_\infty^\infty dx|x\rangle\langle x|\varphi\rangle, \tag{2.5}$$

de modo que operador identidade é um operador de projeção que atua sobre todo o espaço. A referência Toledo Piza (2009), pg.57, nomeia esse operador de *resolução da unidade* em termos da base ortonormal $|x\rangle$. Podemos usar o operador de projeção para reescrever a norma como

$$\|\varphi\| = \langle\varphi|\varphi\rangle^{1/2} = \left(\int_\infty^\infty dx\langle\varphi|x\rangle\langle x|\varphi\rangle\right)^{1/2} = \left(\int_\infty^\infty dx|\varphi\left(x\right)|^2\right)^{1/2} < \infty, \tag{2.6}$$

onde $\langle x|\varphi\rangle = \varphi\left(x\right)$. É interessante notar que o operador projeção é não unitário. Com isso, segundo o postulado II, o sistema deixaria de estar isolado. O que ocorre com o sistema nessa evolução é explicado pelo postulado III.

[8] Ver apêndice C.1.

[9] Ver apêndice C.2.

[10] Alguns autores definem a equação de Schrödinger como um postulado. Veja por exemplo a referência Cohen-Tannoudji et al. (2006), página 222.

Postulado III. *A medida em um sistema quântico S é descrita por uma coleção $\{\hat{M}_m\}$ de operadores de medida, definidos como operadores atuando no espaço de Hilbert H_S associado a S e satisfazendo a relação de completeza*

$$\sum_m \hat{M}_m^\dagger \hat{M}_m = \hat{1}, \tag{2.7}$$

onde $\hat{1}$ é o operador identidade que atua em H_S. O índice m refere-se aos resultados de medição que possam ocorrer no experimento. A probabilidade $p(m)$ de se obter o resultado m, se o sistema estiver no estado $|\psi\rangle$ imediatamente antes da medição é

$$p(m) = \langle\psi|\hat{M}_m^\dagger \hat{M}_M|\psi\rangle, \tag{2.8}$$

e o estado imediatamente após o conhecimento da medida se torna (Julien, 2008, pg.12)

$$\frac{\hat{M}_m|\psi\rangle}{\sqrt{p(m)}}. \tag{2.9}$$

O terceiro postulado cria uma regra de correspondência entre um tipo especifico de operadores, que são denominados operadores de medida, e o ato de se obter informação de um sistema, ou seja, realizar uma medida sobre sistema. Ao criar essa regra de correspondência, vemos que ao somarmos sobre todas as possíveis medidas do sistema obtemos

$$\sum_m p(m) = \sum_m \langle\psi|\hat{M}_m^\dagger \hat{M}_m|\psi\rangle = \langle\psi|\psi\rangle = 1, \tag{2.10}$$

uma vez que o postulado I descreve o estado físico como representado por um raio unitário. Logo, a relação de completeza expressa o fato de que a soma das probabilidades das possíveis medidas deve ser igual a 1. O tipo de medidas que trataremos nesta Tese é chamada de medida projetiva ou medida de von Neumann. Esse tipo de medida pode ser vista como um caso especial das medidas descritas no postulado III. Uma medida projetiva é descrita por um operador auto adjunto, $\hat{M}$, que recebe o nome de *observável*. Este operador possui uma decomposição espectral $\hat{M} = \sum_m m\hat{P}_m$, onde $\hat{P}_m$ é o projetor sobre o auto espaço de $\hat{M}$, com autovalor m (Nielsen and Chuang, 2004, pg.117). Os possíveis resultados da medida correspondem aos autovalores m do observável. Supondo que o sistema se encontre no estado $|\psi\rangle$ imediatamente antes da medida, a probabilidade de obter o resultado m será dada por $p\,(m) = \langle\psi|\hat{P}_m|\psi\rangle$. O estado imediatamente após a medida será $\hat{P}_m|\psi\rangle/\sqrt{p(m)}$.

A probabilidade definida em termos de projetores tem uma importante consequência. Consideremos dois estados $|\psi\rangle$ e $|\phi\rangle$, tal que, $|\psi\rangle = e^{i\theta}|\phi\rangle$, onde θ pertence ao

conjunto dos números reais. Logo,

$$\langle\psi|\hat{P}_m|\psi\rangle = \langle\phi|e^{-i\theta}\hat{P}_m e^{i\theta}|\phi\rangle = \langle\phi|\hat{P}_m|\phi\rangle. \tag{2.11}$$

As probabilidades previstas para uma medida arbitrária são os mesmos para $|\psi\rangle$ e $|\phi\rangle$. Ou seja, a fase global não afeta as predições físicas. Isso justifica a definição de estado físico do postulado I, como um *raio* unitário no espaço de Hilbert.

As medidas em mecânica quântica possuem um carácter estatístico, de modo que as análises dos resultados devem ser feitas em termos do valor médio. Por definição (Nielsen and Chuang, 2004, pg.654) o valor médio de uma medida é

$$\langle\hat{M}\rangle = \sum_m mp\,(m) = \sum_m m\langle\psi|\hat{P}_m|\psi\rangle = \langle\psi|\left(\sum_m m\hat{P}_m\right)|\psi\rangle = \langle\psi|\hat{M}|\psi\rangle. \tag{2.12}$$

A variância associada às medidas do observável $\hat{M}$ pode ser escrita como

$$[\Delta(\hat{M})]^2 = \langle\hat{M}^2\rangle - \langle\hat{M}\rangle^2. \tag{2.13}$$

Portanto, ao serem realizados um grande número de experimentos em que o estado $|\psi\rangle$ foi preparado, e o observável $\hat{M}$ é medido, obtemos resultados com o valor médio $\langle\hat{M}\rangle$ e desvio padrão $\Delta\hat{M}$. A análise dos resultados das medidas para mais de um observável resulta no que talvez seja o resultado mais conhecido da mecânica quântica, o *princípio de incerteza de Heisenberg*. Para ilustrarmos esse princípio, vamos considerar os operadores $\hat{P}$ e $\hat{Q}$ definidos por $\hat{P} = \hat{A} - \langle\hat{A}\rangle$ e $\hat{Q} = \hat{B} - \langle\hat{B}\rangle$. Usaremos também a relação matemática

$$|\langle\psi|[\hat{P},\hat{Q}]|\psi\rangle|^2 + |\langle\psi|\{\hat{P},\hat{Q}\}|\psi\rangle|^2 = 4|\langle\psi|\hat{P}\hat{Q}|\psi\rangle|^2, \tag{2.14}$$

onde $\{\hat{P},\hat{Q}\} = \hat{P}\hat{Q} + \hat{Q}\hat{P}$ é o anti-comutador.

Usando a desigualdade de Schwarz, eq. (2.1), temos

$$|\langle\psi|\hat{P}\hat{Q}|\psi\rangle|^2 \leq \langle\psi|\hat{P}^2|\psi\rangle\langle\psi|\hat{Q}^2|\psi\rangle. \tag{2.15}$$

Inserindo a relação (2.14) em (2.15) temos por sua vez

$$|\langle\psi|[\hat{P},\hat{Q}]|\psi\rangle|^2 + |\langle\psi|\{\hat{P},\hat{Q}\}|\psi\rangle|^2 \leq 4\langle\psi|\hat{P}^2|\psi\rangle\langle\psi|\hat{Q}^2|\psi\rangle.$$

Se eliminarmos o termo do anti-comutador a relação continua válida e a desigualdade se torna mais forte. Logo

$$\langle\psi|\hat{P}^2|\psi\rangle\langle\psi|\hat{Q}^2|\psi\rangle \geq \frac{|\langle\psi|[\hat{P},\hat{Q}]|\psi\rangle|^2}{4}. \tag{2.16}$$

Pelas definições de $\hat{P}$ e $\hat{Q}$ temos $[\hat{P}, \hat{Q}] = [\hat{A}, \hat{B}]$, $\langle \hat{P}^2 \rangle = (\Delta \hat{A})^2$ e $\langle \hat{Q}^2 \rangle = (\Delta \hat{B})^2$, de modo que a relação de incerteza de Heisenberg é dada por

$$(\Delta \hat{A})^2 (\Delta \hat{B})^2 \geq \frac{|\langle \psi | [\hat{A}, \hat{B}] | \psi \rangle|^2}{4}. \tag{2.17}$$

Heisenberg inicialmente concebeu essa relação para os operadores posição e o momento. Substituindo os operadores pelos operadores de posição e momento, e usando a relação $[\hat{x}, \hat{p}] = i\hbar$, deduzida no apêndice D, temos que a relação de incerteza para esses operadores é dada por

$$\Delta \hat{x} \Delta \hat{p} \geq \frac{\hbar}{2} = \frac{1}{4}. \tag{2.18}$$

A última igualdade vem da escolha $\hbar = 1/2$ (Braunstein and van Loock, 2005, pg.516), muito utilizada na área de informação quântica em variáveis continuas. O princípio de Heisenberg nos diz que dado dois observáveis que não comutam $\hat{A}$ e $\hat{B}$, há um limite intrínseco de precisão da medição simultânea de ambos. A medida de um observável necessariamente perturba o outro. Quando os observáveis comutam $[\hat{A}, \hat{B}] = 0$, esses observáveis formam uma conjunto completo de observáveis compatíveis, ou seja, eles possuem um conjunto de autovetores que os diagonalizam simultaneamente (Galindo et al., 2012, pg.55).

Para um sistema físico composto por mais de um subsistema, devemos especificar como devemos descrever o sistema total a partir da descrição dos subsistemas. Dessa forma, precisamos do postulado IV.

Postulado IV *O espaço de Hilbert associado a um sistema físico composto, formado por dois subsistemas A e B, é o produto tensorial $H_A \otimes H_B$ dos espaços de Hilbert H_A e H_B associados com A e B. Portanto, se A é preparado no estado $|\psi_A\rangle$ e B é preparado no estado $|\psi_B\rangle$, o estado do sistema compostos AB é descrito pelo produto tensorial $|\psi_A\rangle \otimes |\psi_B\rangle$, algumas vezes denotado pela notação $|\psi_A\rangle|\psi_B\rangle$ ou $|\psi_A, \psi_B\rangle$* (Julien, 2008, pg.12).

O postulado IV é uma extensão do postulado I, que nos diz como lidar com um sistema composto. Note que todos os postulados anteriores permanecem válidos. A atuação de operadores sobre os estados (tanto de evolução ou medida) seguem a mesma regra imposta pelos postulados II e III. Assim, para sistemas compostos esses operadores poderão atuar em uma parte do sistema (A ou B) ou em todo o sistema AB.

Ao estudarmos um sistema composto podemos nos deparar com estados onde não possuímos o máximo de informação sobre o sistema (Galindo et al., 2012, pg.57), possuindo apenas informação parcial sobre o sistema. Esses estados são denominados estados mistos. Um exemplo de estado misto é um estado onde sabemos as probabilidades p_1, p_2, p_3,. . . ,p_n,. . . de que o estado pode ser encontrado no estado puro representado pelos

vetores $|\psi_1\rangle$, $|\psi_2\rangle$, $|\psi_3\rangle$,...,$|\psi_n\rangle$,..., respectivamente (os quais não são necessariamente ortogonais). Logo, temos que $\sum_i p_i = 1$ e para todos os valores do índice i, $0 \leq p_i \leq 1$. Se $p_n = 1$, e portanto $p_i = 0$ para todo $i \neq n$, então o estado misto é justamente um estado puro. Em geral, é conveniente descrever o estado misto por meio do *operador densidade* ou *matriz densidade* ρ, definida (Galindo et al., 2012, pg.58) como se segue

$$\hat{\rho} \equiv \sum_i p_i |\psi_i\rangle\langle\psi_i|, \tag{2.19}$$

onde p_i é a probabilidade do sistema ser encontrado no estado $|\psi_i\rangle$. Obviamente essa nova descrição do estado de um sistema está de acordo com os outros postulados. Se inicialmente o sistema estiver no estado $|\psi_i\rangle$ com probabilidade p_i, então após a evolução o sistema estará em $\hat{U}|\psi_i\rangle$. Logo a evolução do operador densidade será $\sum_i p_i \hat{U}|\psi_i\rangle\langle\psi_i|\hat{U}^\dagger = \hat{U}\hat{\rho}\hat{U}^\dagger$. O postulado da medida também pode ser descrito em termos do operador densidade, sendo a medida descrita por operadores $\hat{M}_m$. Se o estado imediatamente antes da medida é dado por $|\psi_i\rangle$, a probabilidade de se obter m como resultando será $p(m|i) = \langle\psi_i|\hat{M}^\dagger\hat{M}|\psi_i\rangle = tr\left(\hat{M}_m^\dagger\hat{M}_m|\psi_i\rangle\langle\psi_i|\right)$, onde $p(m|i)$ é a probabilidade condicional de se obter m dado i e tr é a função traço (Nielsen and Chuang, 2004, pg.105). Assim, a probabilidade de se obter m é dada por

$$p(m) \;=\; \sum_i p(m|i)\, p_i = tr\left(\hat{M}^\dagger\hat{M}\rho\right). \tag{2.20}$$

Sendo o estado $|\psi\rangle$ o estado imediatamente antes da medida, o estado após o conhecimento da medida é

$$|\psi_i^m\rangle = \frac{\hat{M}_m|\psi_i\rangle}{\sqrt{\langle\psi_i|\hat{M}_m^\dagger\hat{M}_m|\psi_i\rangle}}. \tag{2.21}$$

Assim, após a medida o operador densidade é composto por estados $|\psi_i^m\rangle$ com respectivas probabilidades $p(i|m)$. Portanto

$$\hat{\rho}^m = \sum_i p(i|m)|\psi_i^m\rangle\langle\psi_i^m| = \sum_i p(i)\frac{\hat{M}_m|\psi_i\rangle\langle\psi_i|\hat{M}_m^\dagger}{\langle\psi_i|\hat{M}_m^\dagger\hat{M}_m|\psi_i\rangle}, \tag{2.22}$$

onde de acordo com a teoria das probabilidades $p(i|m) = p(m|i)\,p(i)\,/p(m)$ (Nielsen and Chuang, 2004, pg.653). Logo, usando as equações (2.20) e (2.21) temos

$$\hat{\rho}^m = \sum_i p_i \frac{\hat{M}_m|\psi_i\rangle\langle\psi_i|\hat{M}_m^\dagger}{tr\left(\hat{M}_m^\dagger\hat{M}_m\hat{\rho}\right)} = \frac{\hat{M}_m\hat{\rho}\hat{M}_m^\dagger}{tr\left(\hat{M}_m^\dagger\hat{M}_m\hat{\rho}\right)}. \tag{2.23}$$

O operador densidade é extremamente útil. Por exemplo, podemos verificar se o estado

é puro ou misto calculando a função traço do operador densidade ao quadrado, $tr\,(\hat{\rho}^2)$. Para um estado puro $tr\,(\hat{\rho}^2) = 1$ e para um estado misto $tr\,(\hat{\rho}^2) < 1$.

Nessa seção procuramos estabelecer os alicerces da mecânica quântica, apresentando seus postulados, com os quais toda a mecânica quântica pode ser construída. O uso sistemático desses quatro postulados é suficiente para derivarmos algumas interessantes propriedades da mecânica quântica e consequentemente da informação quântica. Nas próximas seções vamos explorar outras importantes consequências destes postulados que estão relacionados com o tema dessa Tese.

2.2 Copiando estados quânticos

Uma das divergências mais acentuadas entre a teoria clássica e quântica da informação reside na questão de copiar (clonar) um estado arbitrário. Estados clássicos arbitrários podem ser copiados mas o mesmo não acontece com estados quânticos. Essa impossibilidade foi demostrada por Wootters and Zurek (1982), e leva o nome de *teorema da não-clonagem*, o qual pode ser enunciado da seguinte forma (Benenti et al., 2004, pg.196)

Teorema da não-Clonagem: "*É impossível construir uma máquina universal capaz de copiar estados quânticos arbitrários.*"

Vamos supor que tal máquina exista. Ao receber o estado a ser clonado ela implementa uma transformação unitária $\hat{U}$ que tem como saída dois estados idênticos. Desse modo, para dois estados *distintos* de entrada $|\psi_1\rangle$ e $|\psi_2\rangle$ temos

$$\hat{U}\left(|\psi_1\rangle \otimes |\phi\rangle\right) = |\psi_1\rangle \otimes |\psi_1\rangle, \tag{2.24}$$

$$\hat{U}\left(|\psi_2\rangle \otimes |\phi\rangle\right) = |\psi_2\rangle \otimes |\psi_2\rangle, \tag{2.25}$$

onde $|\phi\rangle$ é o estado inicial auxiliar fornecido pela máquina de clonagem. Calculando o produto escalar entre (2.24) e (2.25),

$$\begin{aligned} \langle\psi_1|\psi_2\rangle\langle\phi|\phi\rangle &= \langle\psi_1|\psi_2\rangle\langle\psi_1|\psi_2\rangle, \\ \langle\psi_1|\psi_2\rangle &= \langle\psi_1|\psi_2\rangle\langle\psi_1|\psi_2\rangle. \end{aligned} \tag{2.26}$$

Existem duas possibilidades que devemos examinar. A primeira é tal que $\langle\psi_1|\psi_2\rangle \neq 0$, o que implica necessariamente $\langle\psi_1|\psi_2\rangle = 1$. Ou seja, $|\psi_1\rangle = |\psi_2\rangle$, contradizendo a hipótese inicial de que os estados são distintos. A segunda possibilidade é tal que $\langle\psi_1|\psi_2\rangle = 0$, implicando que $|\psi_1\rangle$ e $|\psi_2\rangle$ são estados ortogonais. Assim, podemos apenas clonar estados ortogonais, não existindo então uma máquina quântica que possa clonar estados quânticos arbitrários. O fato de o teorema permitir apenas a clonagem de estados ortogonais está de acordo com a possibilidade de clonagem de estados clássicos, pois estados clássicos

distintos são ortogonais (Rigolin, 2005, pg.153).

2.3 Emaranhamento

Muitas características interessantes da mecânica quântica podem ser derivadas a partir de seus postulados. No entanto, uma em especial merece maior atenção devido ao seu papel nesta Tese. Suponha, por exemplo, que preparemos dois fótons A e B com polarizações vertical e horizontal. Denotamos as polarizações por $|0\rangle$ (vertical) e $|1\rangle$ (horizontal). De acordo com o postulado IV, esse sistema é descrito pelo produto tensorial $|0\rangle_A|1\rangle_B$. Por outro lado, se escolhermos preparar dois fótons nas polarizações horizontal e vertical, o estado quântico será descrito por $|1\rangle_A|0\rangle_B$. Agora, lembrando que a mecânica quântica permite a superposição linear, o estado abaixo também representa um estado físico:

$$|\Psi^+\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle_A|1\rangle_B + |1\rangle_A|0\rangle_B\right). \tag{2.27}$$

Esse estado não pode ser escrito como um produto tensorial de dois estados, ou seja, não existe uma descrição $|a\rangle_A$ e $|b\rangle_B$ dos sistemas A e B de modo que possamos escrever $|\Psi^+\rangle = |a\rangle_A|b\rangle_B$. Mesmo que o sistema em questão seja formado por dois fótons, esses não podem ser considerados separadamente pois eles formam uma entidade comum, ou seja, eles estão *emaranhados*. Isso nos leva à seguinte definição (Rigolin, 2005, pg.6)

Definição 1 *Seja um sistema quântico composto de N subsistemas tal que o espaço de Hilbert associado a ele é* $H = \bigotimes_{j=1}^{N} H_j$*, onde* H_j *é o espaço de Hilbert associado a cada subsistema. Se* $|\Psi\rangle \in H$ *é o estado que descreve este sistema, então ele não está emaranhado se, e somente se, podemos escrevê-lo como* $|\Psi\rangle = \bigotimes_{j=1}^{N} |\psi_j\rangle$*, onde* $|\psi_j\rangle \in H_j$*.*

Note que com a nossa definição expandimos o conceito de emaranhamento para estados composto de N partes. Estados emaranhados podem ser classificados de acordo com o número de partes que os constituem (Rigolin, 2005, pg.5). Por exemplo, o estado (2.27)[11] é classificado como estado bipartite. A medida que se aumenta o número de subsistemas modificamos a notação. Para um sistema formado por três subsistemas emaranhados usamos a terminologia tripartite e para sistemas com maior número de subsistemas dizemos emaranhamento multipartite.

Historicamente a noção de emaranhamento (do original em alemão Verschränkung) apareceu explicitamente pela primeira vez na literatura em 1935 (Schrödinger, 1935), sem nenhuma referência a variáveis discretas. De fato, o estado emaranhado tratado por Einstein, Podolsky, e Rosen (Einstein et al., 1935) era constituído por um estado de duas partículas emaranhadas nas variáveis posição e momento, modernamente chamado

[11] O estado (2.27) é conhecido como estado de Bell.

de emaranhamento de variáveis contínuas. Einstein, Podolsky e Rosen consideraram o estado comprimido de dois modos[12]

$$\left(\frac{2}{\pi}\right)^{\frac{1}{2}} \int dx_1 dx_2 \exp\left\{\left[-\frac{e^{2r}}{2}\left[(x_1-x_2)^2\right]-\frac{e^{-2r}}{2}\left[(x_1+x_2)^2\right]\right]\right\}|x_1,x_2\rangle\,, \tag{2.28}$$

com parâmetro de compressão infinito ($r \to \infty$). Com esta escolha para r o estado acima pode ser escrito como (Braunstein and van Loock, 2005, pg.524),

$$\int dx_1 dx_2 \delta\left(x_1-x_2-u\right)|x_1,x_2\rangle \propto \int dx\,|x,x-u\rangle\,, \tag{2.29}$$

descrevendo posições ($x_1-x_2=u$) e momentos ($p_1+p_2=0$) perfeitamente correlacionados (maximamente emaranhados). Esse tipo de estado é conhecido como estado EPR[13]. Entretanto, desprezando o caso limite e considerando o parâmetro de compressão r finito, de modo que as posições e os momentos estão parcialmente correlacionados (emaranhados), esse estado (2.28) continua sendo um estado fisicamente possível de ser implementado experimentalmente.

Uma vez que um estado pode estar parcialmente emaranhado, necessitamos de uma maneira para mensurar sua quantidade de emaranhamento. Para estados puros bipartites podemos mensurar esse emaranhamento através da entropia de von Neumann do estado reduzido (Rigolin, 2005, pg.72) . Se $\rho = |\psi\rangle\langle\psi|$ é o operador densidade que descreve nosso estado puro, a quantidade de emaranhamento de ρ é

$$E\left(\psi\right) = -tr\{\rho_1 \log_2\left(\rho_1\right)\} = -tr\{\rho_2 \log_2\left(\rho_2\right)\}, \tag{2.30}$$

onde $\rho_1 = tr_2\{\rho\}$ e $\rho_2 = tr_1\{\rho\}$ são operadores densidade reduzidos do sistema bipartite. Alguns autores, como por exemplo Braunstein and van Loock (2005) definem a entropia de von Neumann com o logaritmo na base neperiana para mensurar emaranhamento em variáveis contínuas. A razão para não procedermos da mesma maneira é que desejamos ter um parâmetro único de comparação que abrangerá estados puros, descritos por variáveis discretas ou contínuas (Kogias et al., 2014). Por exemplo, podemos calcular a quantidade de emaranhamento do estado (2.27) e comparar com o estado (2.28). Para o estado (2.27) a entropia de von Neumann (2.30) resulta $E\left(\psi^+\right) = 1$ ebit, onde ebit é a unidade de emaranhamento do sistema (Rigolin, 2005, pg.72). Para o estado comprimido (EC) dado pela eq. (2.28),

$$E\left(EC\right) = \cosh^2\left(r\right)\log_2\left(\cosh^2\left(r\right)\right) - \sinh^2\left(r\right)\log_2\left(\sinh^2\left(r\right)\right). \tag{2.31}$$

Note que a quantidade de emaranhamento depende do parâmetro de compressão e para

[12] Veja apêndice E para a dedução.

[13] Esse estado não é físico, não podendo ser criado no laboratório uma vez que possui norma infinita.

obtermos 1 ebit necessitamos de um parâmetro de compressão $r \approx 0.52$, ou $r \approx 4.5$ dB[14]. Para mensurar a quantidade de emaranhamento em estados mistos, usa-se o emaranhamento de formação. Esse se reduz a entropia de von Neumann para estados puros (Rigolin, 2005, pg.82). Nesta Tese usaremos apenas estados emaranhados puros de maneira que apenas o formalismo da entropia de von Neumann se faz necessário.

2.4 Teletransporte

Nessa seção iremos discutir o que na minha opinião é a mais espantosa aplicação da mecânica quântica. Descoberto por Bennett et al. (1993) em 1993 e nomeado como *teletransporte quântico*, essa maravilha quântica pode transmitir a função de onda de um estado a outro através de um estado emaranhado (canal) e informação clássica. Vamos nos ater aqui somente ao protocolo de teletransporte em variáveis discretas, como feito em Rigolin (2005), deixando a extensão para variáveis contínuas para o próximo capítulo. Para uma descrição mais clara iremos fazer uso de dois personagens fictícios, chamados Alice e Bob. Alice e Bob inicialmente compartilham um estado bipartite maximamente emaranhado, o estado de Bell $|\Psi^-\rangle = \left(1/\sqrt{2}\right)(|01\rangle - |10\rangle))$. Esse estado emaranhado é o canal quântico (ou canal EPR) usado para a realização do teletransporte. Alice por sua vez deseja teletransportar o estado desconhecido (qbit ou qubit) $|\phi\rangle = a|0\rangle + b|1\rangle$, onde $|a|^2 + |b|^2 = 1$. O estado composto pelo qbit e pelo canal EPR é escrito, de acordo com o quarto postulado, como

$$|\Phi\rangle \;=\; |\phi\rangle \otimes |\Psi^-\rangle = \frac{a}{\sqrt{2}}\left(|001\rangle - |010\rangle\right) + \frac{b}{\sqrt{2}}\left(|101\rangle - |110\rangle\right), \tag{2.32}$$

onde, por convenção, os dois primeiros qbits pertencem a Alice e o terceiro a Bob ($|AAB\rangle$, onde A pertence a Alice e B a Bob). Podemos reescrever a equação (2.32) em termos dos quatro estados de Bell $|\Psi^\pm\rangle = (1/\sqrt{2})(|01\rangle \pm |10\rangle)$ e $|\Phi^\pm\rangle = (1/\sqrt{2})(|00\rangle \pm |11\rangle)$,

$$\begin{aligned} |\Phi\rangle \;=\; & \frac{1}{2}\{|\Psi^-\rangle\left(-a|0\rangle - b|1\rangle\right) + |\Psi^+\rangle\left(-a|0\rangle + b|1\rangle\right) + \\ & |\Phi^-\rangle\left(a|1\rangle + b|0\rangle\right) + |\Phi^+\rangle\left(a|1\rangle - b|0\rangle\right). \end{aligned} \tag{2.33}$$

Dando seguimento ao protocolo Alice realiza a medida dos seus estados na base de estados de Bell. De acordo com o terceiro postulado Alice tem 1/4 de chance de obter quaisquer dos quatro estados de Bell. Segundo o terceiro postulado, caso a medida de Alice seja igual $|\Psi^\pm\rangle$ o estado resultante pós medida será $|\Psi^\pm\rangle \otimes (-a|0\rangle \pm b|1\rangle)$; caso a medida forneça $|\Phi^\pm\rangle$, o estado resultante pós medida será $|\Phi^\pm\rangle \otimes (a|1\rangle \mp b|0\rangle)$.

Após a medida, Alice comunica a Bob o resultado utilizando comunicação

[14] Alguns autores preferem mensurar o parâmetro de compressão em termos do decibel, a relação entre as quantidades é dada por $\mathrm{dB} = 10\log_{10}\left(e^{2r}\right)$.

clássica. Bob, de posse dos dois bits de informação provenientes da medida de Alice, sabe em qual dos quatro estados o seu qbit se encontra. Dessa forma, Bob aplica a operação unitária necessária para obter o estado $|\phi\rangle$. Para o resultando da medida de Alice igual a $|\Psi^-\rangle$, Bob não necessita realizar nenhuma operação sobre o seu estado e isso é indicado através do operador identidade I. Caso o resultado obtido por Alice seja $|\Psi^+\rangle$, Bob aplica sobre seu estado o operador σ_z. Tendo como resultado da medida $|\Phi^-\rangle$, Bob deve aplicar o operador σ_x e por fim caso a medida de Alice venha a ser $|\Phi^+\rangle$, Bob deverá aplicar as operações $\sigma_z\sigma_x$ para recuperar o estado $|\phi\rangle$. Aqui, σ_x, σ_y e σ_z são os operadores (ou matrizes) de Pauli.

O teorema da não-clonagem, seção 2.2, nos garante que o estado outrora pertencente a Alice não pode ser copiado. Para nos certificarmos disso podemos realizar o cálculo do estado com Alice após o fim do protocolo. O estado de Alice após o protocolo é descrito por um dos quatro estados de Bell, $\rho^A_{1,2} = |\Psi^\pm\rangle\langle\Psi^\pm|$ ou $\rho^A_{1,2} = |\Phi^\pm\rangle\langle\Phi^\pm|$. Calculando o traço em relação ao qbit 2 temos $\rho^A_1 = (1/2)\left(|0\rangle\langle 0| + |1\rangle\langle 1|\right)$. Vemos claramente que o estado de Alice é agora uma mistura estatística e não apresenta mais informação sobre o estado original. Logo, ao fim do protocolo o estado outrora com Alice passa a pertencer a Bob e desse modo temos que toda a informação contida no estado é transferida para o estado de Bob usando como recurso o canal EPR e os dois bits de informação clássica.

Há ainda a questão sobre a necessidade dos dois bits de informação clássica para o correto funcionamento do protocolo. Para verificarmos a necessidade dos bits clássicos, podemos calcular o estado de Bob imediatamente antes do recebimento da informação. Tomando o traço sobre os estados de Alice temos $\rho_B = (1/2)\left(|0\rangle\langle 0| + |1\rangle\langle 1|\right)$. Vemos então que o estado de Bob é descrito por uma mistura estatística, não contendo nenhuma informação sobre o estado de Alice. Isso deixa claro a importância da informação clássica para a conclusão do protocolo.

Caso as operações realizadas por Bob não sejam perfeitamente executadas (seja por erro humano ou falta de precisão do equipamento), o estado final com Bob não será exatamente igual ao estado outrora pertencente a Alice. Para verificarmos o quão próximo um estado se encontra do outro devemos usar as chamadas medidas de distância em informação quântica (Nielsen and Chuang, 2004, pg.437).

Na próxima seção estudaremos a fidelidade, a medida de distância entre dois estados quânticos utilizada nesta Tese.

2.5 Fidelidade

A fidelidade é uma medida de distância entre dois estados quânticos. Embora ela não possa ser considerada uma distância do ponto de vista matemático, ela satisfaz algumas condições que justificam o seu uso (Braunstein and van Loock, 2005;

Nielsen and Chuang, 2004). Uma dessas condições é o fato de que a fidelidade F está limitada entre 0 e 1, sendo 0 quando temos estados ortogonais e 1 quando temos dois estados iguais.

Nesta Tese iremos utilizar como estado de entrada apenas estados puros, $\hat{\rho}_{in} = |\psi\rangle_{in in}\langle\psi|$, de modo que a fidelidade pode ser definida como (Braunstein et al., 2000)

$$F\left(|\psi\rangle_{in}, \hat{\rho}_{out}\right) = {}_{in}\langle\psi|\hat{\rho}_{out}|\psi\rangle_{in}, \tag{2.34}$$

onde $\hat{\rho}_{in}$ é o estado com Alice no início do protocolo (ou estado de entrada) e $\hat{\rho}_{out}$ é o estado com Bob no fim do protocolo (ou estado de saída).

Ao manter o estado de saída da forma mais geral possível, estamos supondo que durante o protocolo pode ocorrer decoerência que leve o estado de Bob para um estado misto. Caso o estado de saída seja um estado puro, a fidelidade pode ser reescrita como

$$F\left(|\psi\rangle_{in}, |\phi\rangle_{out}\right) = |{}_{in}\langle\psi|\phi\rangle_{out}|^2. \tag{2.35}$$

A fidelidade mede o quão "próximo" o estado de saída está do estado de entrada após, por exemplo, a realização do teletransporte. Caso desejemos teletransportar um conjunto de estados (ensemble), devemos tomar a média sobre todos os possíveis resultados de medidas para o ensemble de entrada, de modo que o operador densidade que define o estado de saída será um operador densidade médio. Para um ensemble de estados puros ele pode ser escrito como (Braunstein and van Loock, 2005, pg.543)

$$\hat{\rho}_M = \int_{-\infty}^{\infty}\int_{-\infty}^{\infty} d\tilde{x}_1 d\tilde{x}_2 \mathbb{P}(\tilde{x}_1, \tilde{x}_2) |\phi\left(\tilde{x}_1, \tilde{x}_2\right)\rangle_{out out}\langle\phi\left(\tilde{x}_1, \tilde{x}_2\right)|, \tag{2.36}$$

onde $\tilde{x}_1$ e $\tilde{x}_2$ são as medidas realizadas por Alice e $\mathbb{P}(\tilde{x}_1, \tilde{x}_2)$ é a probabilidade de realizar essas medidas. Note que a equação acima é valida para um estado de saída puro $|\phi\left(\tilde{x}_1, \tilde{x}_2\right)\rangle_{out}$. Para um estado misto basta escrevermos a expressão acima em termos do operador densidade. Supomos também que o estado possui um espectro contínuo, de modo que escrevemos o estado na base da posição. Caso o estado seja discreto podemos reescrever em outra base de modo que a integral se tornará uma somatória. Usando as equações (2.34) e (2.36), a fidelidade para o teletransporte de um ensemble pode ser escrito como

$$F\left(|\psi\rangle_{in}, \hat{\rho}_M\right) = \int_{-\infty}^{\infty}\int_{-\infty}^{\infty} d\tilde{x}_1 d\tilde{x}_2 \mathbb{P}\left(\tilde{x}_1, \tilde{x}_2\right) F\left(|\psi\rangle_{in}, \hat{\rho}_{out}\left(\tilde{x}_1, \tilde{x}_2\right)\right), \tag{2.37}$$

onde $\mathbb{P}\left(\tilde{x}_1, \tilde{x}_2\right)$ é a probabilidade de medida dos estados de Alice. Note que deixamos explícito a dependência de $\hat{\rho}_{out}$ com os resultados das medidas de Alice. Supondo que Alice e Bob saibam que o estado teletransportado pertença a um conjunto fixo de estados,

podemos definir uma fidelidade levando em conta essa informação (Braunstein et al., 2000),

$$F_m = \int d|\psi\rangle_{in} P\left(|\psi\rangle_{in}\right) F\left(|\psi\rangle_{in}, \hat{\rho}_M\right), \tag{2.38}$$

onde $P\left(|\psi\rangle_{in}\right)$ é a distribuição de probabilidade do estado de entrada e a integral percorre todo o conjunto de estados de entrada. Se o conjunto de estados de entrada contém todos os possíveis estados quânticos no espaço de Hilbert de dimensão infinita, a melhor fidelidade média F_m alcançável por Alice e Bob sem o uso de emaranhamento é zero. O correspondente da fidelidade média sem o uso de emaranhamento para um espaço de Hilbert d-dimensional é $F_m = 2/\left(1+d\right)$ (Barnum, 1998). Assim, obtém-se $F_m = 0$ para $d \to \infty$. Ao considerarmos $d = 2$, ou seja, o espaço de Hilbert de um qbit, o valor máximo da fidelidade média na ausência de emaranhamento é dada por $F_m = 2/3$. Se restringirmos o estado de entrada, considerando apenas os estados coerentes com amplitude α, a fidelidade média possível levando em conta apenas recursos clássicos e considerando a distribuição sobre todo plano complexo do estado coerente é limitada por $F_m = 1/2$. Dada a facilidade do cálculo e fácil interpretação, a fidelidade é uma medida de distância amplamente utilizada na teoria da informação em variáveis contínuas (Braunstein and van Loock, 2005; Furusawa et al., 1998; Lee et al., 2011).

Até a presente seção nos dedicamos aos postulados da mecânica quântica e suas consequências mais importantes para a teoria da informação quântica. A partir da próxima seção iremos particularizar nossa análise para sistemas ópticos.

2.6 Variáveis contínuas em óptica quântica

Nessa seção investigaremos as possibilidades oferecidas pela óptica de variáveis contínuas para a execução de comunicação quântica. Por óptica, queremos dizer que os sistemas físicos utilizados para transportar informação são estados quânticos do campo eletromagnético. O termo variáveis contínuas, por outro lado, refere-se aos espectros contínuos dos observáveis utilizados para descrever o estado quântico que transportarão a informação. A aplicação da mecânica quântica para caracterizar as propriedades da luz é conhecida como óptica quântica.

Em óptica quântica, os modos eletromagnéticos quantizados correspondem a osciladores harmônicos quânticos. O Hamiltoniano que descreve um oscilador harmônico quântico pode ser expresso em termos dos operadores de criação e aniquilação, $\hat{H}_k = \hbar\omega_k\left(\hat{a}^\dagger\hat{a} + 1/2\right)$ onde k representa um modo do campo eletromagnético (Orszag, 2007, pg.24). Podemos reescrever o Hamiltoniano em termos dos operadores de posição e mo-

mento,

$$\hat{H}_k = \frac{1}{2}\left(\hat{p}_k^2 + \omega_k^2 \hat{x}_k^2\right), \tag{2.39}$$

onde

$$\hat{x}_k = \sqrt{\frac{\hbar}{2\omega_k}}\left(\hat{a}_k + \hat{a}_k^\dagger\right) \quad e \quad \hat{p}_k = -i\sqrt{\frac{\hbar\omega_k}{2}}\left(\hat{a}_k - \hat{a}_k^\dagger\right). \tag{2.40}$$

Aqui usamos a relação de comutação da posição com o momento $[\hat{x}_k, \hat{p}_k] = i\hbar$, a qual é consistente com a relação de comutação bosônica $[\hat{a}_k, \hat{a}_{k'}^\dagger] = \delta_{kk'}$, $[\hat{a}_k, \hat{a}_{k'}] = 0$ (Braunstein and van Loock, 2005, pg.516). Nas equações (2.40), podemos ver que os operadores posição e momento estão relacionados com as partes reais e imaginárias dos operadores de aniquilação e criação. Assim, podemos definir o par de variáveis conjugadas

$$\hat{X}_k \equiv \sqrt{\frac{\omega_k}{2\hbar}}\hat{x}_k = Re\left[\hat{\alpha}\right], \quad \hat{P}_k \equiv \frac{1}{\sqrt{2\hbar\omega_k}}\hat{p}_k = Im\left[\hat{\alpha}_k\right], \tag{2.41}$$

onde

$$\left[\hat{X}_k, \hat{P}_{k'}\right] = \frac{i}{2}\delta_{kk'}. \tag{2.42}$$

Esses novos operadores de posição e momento adimensionais possuem a mesma relação de comutação de (D.1) se definirmos $\hbar = 1/2$. Esses operadores representam as quadraturas de um único modo k e em termos clássicos correspondem a parte real e imaginária da amplitude complexa de um oscilador. Daqui para frente usaremos $(\hat{X}, \hat{P})$ ou $(\hat{x}, \hat{p})$ para nos referirmos as quadraturas adimensionais que farão o papel de posição e momento.

Para fixar as ideias, vamos olhar um campo elétrico de um único modo de frequência e para uma única polarização (Julien, 2008, pg.20),(Braunstein and van Loock, 2005, pg.517)

$$\hat{E}\left(\mathbf{r}, t\right) = E_0\left[\hat{a}_k e^{i(\mathbf{k}\cdot\mathbf{r}-\omega_k t)} + \hat{a}_k^\dagger e^{-i(\mathbf{k}\cdot\mathbf{r}-\omega_k t)}\right], \tag{2.43}$$

onde a contante E_0 contém todos os parâmetros dimensionais. Usando as relações

$$\hat{x}_k = \left(\hat{a}_k + \hat{a}_k^\dagger\right)/2, \quad \hat{p}_k = \left(\hat{a}_k - \hat{a}_k^\dagger\right)/2i, \tag{2.44}$$

podemos escrever o campo elétrico em termos da posição e momento

$$\hat{E}_k\left(\mathbf{r}, t\right) = 2E_0\left[\hat{x}_k \cos\left(\omega_k t - \mathbf{k}\cdot\mathbf{r}\right) + \hat{p}_k \sin\left(\omega_k t - \mathbf{k}\cdot\mathbf{r}\right)\right]. \tag{2.45}$$

Os auto-estados dos operadores de quadratura (Braunstein and van Loock, 2005, pg.517)

de um único modo são

$$\hat{x}|x\rangle = x|x\rangle, \quad \hat{p}|p\rangle = p|p\rangle, \tag{2.46}$$

onde omitimos o índice k. Os auto-estados dos operadores de quadratura são ortogonais,

$$\langle x|x'\rangle = \delta\left(x - x'\right), \quad \langle p|p'\rangle = \delta\left(p - p'\right), \tag{2.47}$$

e completos

$$\int_{-\infty}^{\infty} |x\rangle\langle x| dx = 1, \quad \int_{-\infty}^{\infty} |p\rangle\langle p| dp = 1. \tag{2.48}$$

Os auto-estados dos operadores de quadratura são relacionados através de uma transformada de Fourier,

$$|x\rangle = \frac{1}{\sqrt{\pi}} \int_{-\infty}^{\infty} e^{-2ixp}|p\rangle dp, \tag{2.49}$$

$$|p\rangle = \frac{1}{\sqrt{\pi}} \int_{-\infty}^{\infty} e^{2ixp}|x\rangle dx. \tag{2.50}$$

2.6.1 Estados Gaussianos

Um estado Gaussiano é um estado com função característica Gaussiana (também conhecida como função geradora de momentos), sendo portanto completamente caracterizado pelos primeiros e segundos momentos estatístico dos operadores de quadratura (Adesso, 2006, pg.32). Considerando um sistema bipartite composto de dois subsistemas, A e B, consistindo de N e M modos, respectivamente, a função característica que descreve esse sistema por ser escrita como (Giedke et al., 2001)

$$\chi\left(R\right) = tr\left[\hat{\rho}\hat{D}\left(R\right)\right], \tag{2.51}$$

onde $\hat{\rho}$ é operador densidade do estado bipartite, $R = (x_1, p_1, \ldots, x_{N+M}, p_{N+M}) \in \mathbb{R}^{2N+2M}$ é um vetor real e

$$\hat{D}\left(R\right) = e^{-i\sum_k \left(x_k \hat{X}_k + p_k \hat{P}_k\right)}. \tag{2.52}$$

Aqui $\hat{X}_k$ e $\hat{P}_k$ são os operadores de quadratura. A função característica define exclusivamente o estado $\hat{\rho}$ e estamos considerando estados exclusivamente Gaussianos, ou seja, estados para os quais a função característica é uma função Gaussiana de R (Giedke et al., 2001; Rigolin and Escobar, 2004)

$$\chi\left(R\right) = e^{-\frac{1}{4}R^T \gamma R - id^T R}, \tag{2.53}$$

onde γ é a matriz de correlação (MC) e d um vetor real de dimensão $2N+2M$. Os elementos γ_{ij} da MC podem ser calculados diretamente da matriz densidade pela seguinte relação (Rigolin and Escobar, 2004)

$$\gamma_{ij} = tr\left[\left(Q_i Q_j + Q_J Q_i\right)\rho\right] - 2tr\left[Q_i\rho\right] tr\left[Q_j\rho\right], \tag{2.54}$$

onde $Q = (\hat{x}_1, \hat{p}_1 \ldots \hat{x}_{N+M}, \hat{p}_{N+M})$. A MC γ é um estado fisicamente possível se, e somente se, ela for estritamente positiva, real, simétrica e satisfizer a relação (Giedke et al., 2001)

$$\gamma \geq J^T \gamma^{-1} J, \tag{2.55}$$

onde $J_{N+M} = \oplus_{k=1}^{N+M} J_1$, $J_1 = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ e $\oplus$ denota a soma direta de matrizes. Note que a desigualdade acima é para ser entendida como uma relação entre autovalores das matrizes do lado esquerdo e direito.

Alguns exemplos de estados Gaussianos são os estados de vácuo, estados coerente, estados comprimidos e estados térmicos. Aqui, vamos realizar uma análise detalhada dos estados coerentes e dos estados comprimidos, visto que esses estados serão os mais utilizados nesta Tese.

Estados coerentes

Descobertos por Schrödinger (Schrödinger, 1926; Steiner, 1988) em 1926, e estudados com detalhes no contexto de campos eletromagnéticos quantizados por R. Glauber (Glauber, 1963), J. Klauder (Klauder, 1960) e E. C. G. Sudarshan (Sudarshan, 1963), os estados coerentes são de importância central em mecânica quântica e em particular em óptica quântica. Esses estados podem ser expressos como combinações lineares dos auto-estados do oscilador harmônico e sua função de onda imita da melhor maneira possível o movimento clássico de uma partícula em um potencial quadrático (Schleich, 2001, pg.108). O estado coerente é definido (Orszag, 2007, pg.31)(Glauber, 1963; Sudarshan, 1963) como auto-estado do operador de aniquilação $\hat{a}$. Para um único modo temos

$$\hat{a}|\alpha\rangle = \alpha|\alpha\rangle. \tag{2.56}$$

Como o operador aniquilação não é Hermitiano, α é um número complexo. Uma forma interessante de se obter um estado coerente é utilizando o operador de deslocamento (Glauber, 1963; Sudarshan, 1963)(Orszag, 2007, pg.33)

$$\hat{D}\left(\alpha\right) = e^{\alpha\hat{a}^\dagger - \alpha^*\hat{a}}. \tag{2.57}$$

Podemos reescrever esse operador usando a relação Baker-Campbell-Hausdorff (Orszag, 2007, pg.364),

$$\hat{D}(\alpha) = e^{-\frac{|\alpha|^2}{2}} e^{\alpha \hat{a}^\dagger} e^{-\alpha^* \hat{a}}. \tag{2.58}$$

Aplicando esse operador no estado de vácuo obtemos

$$\hat{D}(\alpha)|0\rangle = |\alpha\rangle. \tag{2.59}$$

Uma representação bastante útil dos estados coerentes é a representação na base de número (ou base dos estados de Fock) (Walls and Milburn, 2008, pg.13). Para realizar essa mudança de base podemos tomar o produto escalar em ambos os lados da equação (2.56) com $\langle n|$ (Glauber, 1963),

$$(n+1)^{1/2}\langle n+1|\alpha\rangle = \alpha\langle n|\alpha\rangle. \tag{2.60}$$

Realizando algumas simplificações temos

$$\langle n|\alpha\rangle = \frac{\alpha^n}{\sqrt{n!}} e^{-\frac{|\alpha|^2}{2}}, \tag{2.61}$$

onde usamos o fato de que $\langle n| = \langle 0|\hat{a}/\sqrt{n!}$ e $\langle 0|\alpha\rangle = \langle 0|\hat{D}(\alpha)|0\rangle = e^{-\frac{|\alpha|^2}{2}}$. Multiplicando o estado coerente por $1 = \sum_n^\infty |n\rangle\langle n|$ obtemos a expansão do estado coerente na base dos estados de número (Fock),

$$|\alpha\rangle = \sum_n^\infty |n\rangle\langle n|\alpha\rangle = e^{-\frac{|\alpha|^2}{2}} \sum_n^\infty \frac{\alpha^n}{\sqrt{n!}}|n\rangle. \tag{2.62}$$

Na base de Fock podemos calcular a distribuição de probabilidade dos fótons em um dado estado coerente,

$$P(n) = |\langle n|\alpha\rangle|^2 = \frac{|\alpha|^{2n} e^{-|\alpha|^2}}{n!}. \tag{2.63}$$

Vemos que é uma distribuição de Poisson com número médio de fótons dado por $|\alpha|^2$ $\left(\bar{n} = \langle\alpha|\hat{a}^\dagger\hat{a}|\alpha\rangle = |\alpha|^2\right)$. Ao usarmos a equação (2.62) podemos verificar com facilidade que o estado coerente é normalizado $|\langle\alpha|\alpha\rangle|^{1/2} = 1$. Embora os estados coerentes sejam normalizados, estes não são ortogonais. Ao realizarmos o produto escalar entre dois estado coerentes diferentes temos

$$\langle\beta|\alpha\rangle = \langle 0|\hat{D}^\dagger(\beta)\hat{D}(\alpha)|0\rangle = e^{-\frac{1}{2}\left(|\alpha|^2+|\beta|^2\right)+\alpha\beta^*}, \tag{2.64}$$

onde usamos a equação (2.58). Vemos que os estados se tornam aproximadamente ortogonais no limite $|\alpha - \beta| \gg 1$. Esse fato é usado por Ralph et al. (2003) para realizar computação quântica com estados coerentes. Uma consequência da equação (2.64) é o fato de que qualquer estado coerente pode ser expandindo em termos de outros estados coerentes, indicando que os estados coerentes são supercompletos.

Uma representação na qual temos particular interesse é a representação na base da posição. Nessa base o estado coerente pode ser escrito como

$$|\alpha\rangle = \int_{-\infty}^{+\infty} dx \phi_\alpha(x) |x\rangle, \tag{2.65}$$

onde a função de onda $\phi(x)$ é dada por

$$\phi_\alpha(x) = \left(\frac{2}{\pi}\right)^{1/4} e^{-x^2+2x\alpha-\frac{\alpha^2}{2}-\frac{|\alpha|^2}{2}}. \tag{2.66}$$

Essa representação será muito útil no cálculo dos protocolos de teletransporte.

O estado coerente é um estado Gaussiano pois a função de onda que o descreve é escrita na base da posição, eq (2.66), é uma função Gaussiana deslocada. Podemos utilizar a equação (2.51) para calcular a função característica do estado coerente,

$$\chi(x,p) = e^{-\frac{1}{4}\left(x^2+p^2\right)-i\frac{x}{2}(\alpha+\alpha^*)-\frac{p}{2}(\alpha-\alpha^*)}, \tag{2.67}$$

onde podemos confirmar seu caráter Gaussiano e, portanto, o fato de o estado coerente ser considerado estado Gaussiano.

O estado coerente também é conhecido como estado de incerteza mínima, ou seja, a variância das quadraturas (equação (2.18)) é a mínima permitida pela mecânica quântica. De fato, usando as equações (2.44) e (2.56) obtemos

$$\langle \hat{x}_k \rangle = \frac{1}{2}\langle\alpha| \left(\hat{a}_k + \hat{a}_k^\dagger\right) |\alpha\rangle = \frac{1}{2}(\alpha + \alpha^*) \tag{2.68}$$

e

$$\langle \hat{x}_k^2 \rangle = \frac{1}{4}\langle\alpha| \left(\hat{a}_k + \hat{a}_k^\dagger\right)^2 |\alpha\rangle = \frac{1}{4}\left(1 + (\alpha + \alpha^*)^2\right). \tag{2.69}$$

Com isso

$$(\Delta\hat{x}_k)^2 = \langle \hat{x}_k^2 \rangle - \langle \hat{x}_k \rangle^2 = \frac{1}{4}. \tag{2.70}$$

Realizando o mesmo procedimento para a outra quadratura temos $(\Delta\hat{p}_k)^2 = 1/4$ e por-

tanto a relação de incerteza fica

$$\Delta\hat{x}_k \Delta\hat{p}_k = \frac{1}{4}. \tag{2.71}$$

Ao compararmos com a relação (2.18) vemos que o estado coerente assume o valor mínimo permitido, sendo então um estado de mínima incerteza. Nesse sentido, o estado coerente é um dos estados quânticos mais próximo de uma descrição clássica do campo eletromagnético (Walls and Milburn, 2008, pg.12).

Estados comprimidos

Como vimos, os estados coerentes são estados de mínima incerteza, com iguais incertezas em ambas quadraturas. Assim como os estados coerentes, existe outra família de estados que também possui incerteza mínima, porém com diferentes incertezas em suas quadraturas. Esses estados são denominados estados comprimidos. Ao lidarmos com emaranhamento na seção 2.3 mencionamos um membro dessa família, o estado comprimido de dois modos dado pela eq. (2.28). Nessa seção vamos estudar esse estado com um pouco mais de detalhe.

O estado coerente comprimido é gerado pelo Hamiltoniana de dois fótons (Scully and Zubairy, 1997, pg.63)

$$\mathcal{H} = i\hbar\left(g\hat{a}^{\dagger 2} - g^{*}\hat{a^{2}}\right), \tag{2.72}$$

onde g é a constante de acoplamento. Podemos definir o operador unitário de compressão (Scully and Zubairy, 1997, pg. 64)

$$\hat{S}\left(\xi\right) = e^{\frac{\xi^{*}}{2}\hat{a}^{2} - \frac{\xi}{2}\hat{a}^{\dagger 2}}, \tag{2.73}$$

onde $\xi = -re^{i\Theta}$ é um número complexo arbitrário e r é conhecido como parâmetro de compressão. O operador de compressão satisfaz a relação $\hat{S}^{\dagger}\left(\xi\right) = \hat{S}^{-1}\left(\xi\right) = \hat{S}\left(-\xi\right)$ e ao atuar sobre os operadores $\hat{a}$ e $\hat{a}^{\dagger}$ dá (Braunstein and van Loock, 2005, pg.521)

$$\begin{aligned} \hat{S}^{\dagger}\left(\xi\right)\hat{a}\hat{S}\left(\xi\right) &= \hat{a}\cosh\left(r\right) + \hat{a}^{\dagger}e^{i\Theta}\sinh\left(r\right), \\ \hat{S}^{\dagger}\left(\xi\right)\hat{a}^{\dagger}\hat{S}\left(\xi\right) &= \hat{a}^{\dagger}\cosh\left(r\right) + \hat{a}e^{-i\Theta}\sinh\left(r\right). \end{aligned} \tag{2.74}$$

Essas relações são extremamente úteis no cálculo das relações de incerteza das quadraturas. Para a quadratura $\hat{x}$ temos

$$\begin{aligned} \langle\hat{x}\rangle &= \langle\alpha|\hat{S}^{\dagger}\left(\xi\right)\frac{\left(\hat{a}+\hat{a}^{\dagger}\right)}{2}\hat{S}\left(\xi\right)|\alpha\rangle = \frac{1}{2}\left[\langle\alpha|\hat{S}^{\dagger}\left(\xi\right)\hat{a}\hat{S}\left(\xi\right)|\alpha\rangle + \langle\alpha|\hat{S}^{\dagger}\left(\xi\right)\hat{a}^{\dagger}\hat{S}\left(\xi\right)|\alpha\rangle\right] \\ &= \frac{1}{2}\left[\alpha\left(\cosh\left(r\right) + e^{-i\Theta}\sinh\left(r\right)\right) + \alpha^{*}\left(\cosh\left(r\right) + e^{i\Theta}\sinh\left(r\right)\right)\right], \end{aligned} \tag{2.75}$$

$$\begin{aligned}\langle\hat{x}^2\rangle &= \langle\alpha|\hat{S}^{\dagger}(\xi)\frac{\left(\hat{a}+\hat{a}^{\dagger}\right)^2}{4}\hat{S}(\xi)|\alpha\rangle \\ &= \frac{1}{4}\Big\{\left[\alpha\left(\cosh(r)+e^{-i\Theta}\sinh(r)\right)+\alpha^*\left(\cosh(r)+e^{i\Theta}\sinh(r)\right)\right]^2+ \\ &\quad 2\cosh(r)\sinh(r)\cos(\Theta)+1+2\sinh^2(r)\Big\}, \end{aligned} \tag{2.76}$$

e portanto

$$(\Delta\hat{x})^2=\langle\hat{x}^2\rangle-\langle\hat{x}\rangle^2=\frac{1}{4}\left[2\cosh(r)\sinh(r)\cos(\Theta)+1+2\sinh^2(r)\right]. \tag{2.77}$$

Alguns autores como (Scully and Zubairy, 1997, pg.65) definem novas quadraturas rotacionadas, de modo a fazer com que o ângulo Θ desapareça. Nós apenas o faremos igual a zero. Com isso

$$(\Delta\hat{x})^2=\frac{1}{4}e^{2r} \quad , \quad (\Delta\hat{p})^2=\frac{1}{4}e^{-2r} \quad \Longrightarrow \quad \Delta\hat{x}\Delta\hat{p}=\frac{1}{4}. \tag{2.78}$$

Como dissemos anteriormente, o estado comprimido é um estado de incerteza mínima. Mas diferentemente do estado coerente, as incertezas em suas quadraturas não são simétricas. A medida que uma incerteza em uma quadratura diminui, a incerteza na outra quadratura aumenta. Quando o parâmetro de compressão tende a infinito $r\to\infty$, temos uma quadratura completamente determinada, incerteza nula, e outra quadratura com incerteza infinita. Porém, esse estado seria um estado não físico (sua norma seria infinita), de modo que com o estado comprimido podemos reduzir a incerteza em uma quadratura mas nunca determiná-la com completa exatidão.

Um estado comprimido de importância nesse trabalho é o estado de vácuo comprimido de dois modos, eq. (2.28). Esse estado pode ser obtido através do operador de compressão de dois modos

$$\hat{S}_2(\xi)=e^{\frac{\xi^*}{2}\hat{a}_1\hat{a}_2-\frac{\xi}{2}\hat{a}_1^{\dagger}\hat{a}_2^{\dagger}}, \tag{2.79}$$

como pode ser visto no apêndice E, com o Hamiltoniano correspondente dado por $\hat{H}=-i\hbar(\xi^*\hat{a}_1\hat{a}_2-\xi\hat{a}_1^{\dagger}\hat{a}_2^{\dagger})$. Esse estado é um estado Gaussiano e sua função característica é

$$\begin{aligned}\chi(x_1,p_1,x_2,p_2) &= \exp\Big\{-\frac{e^{-2r}}{8}\left[(x_1-x_2)^2+(p_1+p_2)^2\right]-\frac{e^{2r}}{8}\left[(x_1+x_2)^2\right. \\ &\quad \left.+(p_1-p_2)^2\right]\Big\}, \end{aligned} \tag{2.80}$$

claramente uma função Gaussiana. Alguns autores (Braunstein and van Loock, 2005; Wang et al., 2007) nomeiam o estado de vácuo comprimido de dois modos de estados EPR ou estados de Bell no espaço de posição-momento sempre que os autovalores dos

operadores $(\hat{x}_1 - \hat{x}_2)$ e $(\hat{p}_1 + \hat{p}_2)$ vão a zero. Essa condição implica uma compressão infinita (ver apêndice E) e um estado maximamente emaranhado.

2.6.2 Operações Gaussianas

Uma operação Gaussiana é uma operação que mapeia um estado Gaussiano de entrada em um estado Gaussiano de saída (Eisert and Plenio, 2003, pg.491). O mapa das operações Gaussianas é um mapa positivo e por isso é completamente descrito por uma transformação simplética sobre a matriz de covariância $\gamma \longmapsto S\gamma S^T$. Como consequência do teorema de Stone-von Neumann (Rosenberg, 2004), dada uma transformação simplética real S existe uma única operação unitária agindo sobre o espaço de estados (Eisert and Plenio, 2003, pg.491). Logo, podemos associar as transformações simpléticas sobre a matriz de covariância, que representam os estados Gaussianos, a operações unitárias.

Algumas dessas operações já foram apresentadas nessa Tese, tais como a operação de deslocamento, eq.(2.58), e a operação de compressão, eq.(2.79). Essas operações são Gaussianas uma vez que aplicadas em um estado Gaussiano retornam outro estado também Gaussiano. Outra operação Gaussiana que será usada nesta Tese é a operação referente ao divisor de feixes (beam splitter). A operação de um divisor de feixes livre de fase (phase-free beam-splitter) é dada simplesmente pela transformação linear abaixo (Braunstein and van Loock, 2005, pg.519)

$$\hat{B}^{\dagger}_{1,2}(\theta)\begin{pmatrix}\hat{a}_1\\ \hat{a}_2\end{pmatrix}\hat{B}_{1,2}(\theta) = \begin{pmatrix}\sin(\theta) & \cos(\theta)\\ \cos(\theta) & -\sin(\theta)\end{pmatrix}\begin{pmatrix}\hat{a}_1\\ \hat{a}_2\end{pmatrix}, \tag{2.81}$$

onde os parâmetros de refletividade e transmitância são dados por $\sin(\theta)$ e $\cos(\theta)$ respectivamente. Na representação de Schrödinger temos $\hat{\rho}' = \hat{B}_{1,2}(\theta)\,\hat{\rho}\hat{B}^{\dagger}_{1,2}(\theta)$, ou simplesmente $|\psi'\rangle = \hat{B}_{1,2}|\psi\rangle$ para um estado puro. Dessa forma a atuação do operador $\hat{B}_{1,2}(\theta)$ na base da posição é (Braunstein and van Loock, 2005, pg.520)

$$\hat{B}_{1,2}(\theta)\,|x_1, x_2\rangle = |x_1\sin(\theta) + x_2\cos(\theta), x_1\cos(\theta) - x_2\sin(\theta)\rangle. \tag{2.82}$$

2.6.3 Detecção homódina

Em mecânica quântica a medida é regida pelo terceiro postulado (veja seção 2.1). Uma das maneiras de se implementar experimentalmente este postulado se dá por meio da técnica de medida chamada detecção homódina balanceada. Esta técnica tem por característica ser uma operação Gaussiana e tem sido amplamente utilizada no âmbito de óptica quântica para realizar medidas das quadraturas do campo eletromagnético (Paul, 2004, pg.160).

Essa técnica consiste em misturar o feixe que se quer analisar, o qual denominamos sinal (fig. 2.1, feixe azul), com um feixe de laser intenso o qual denominamos

oscilador local (fig. 2.1, feixe vermelho). A combinação desses feixes é realizada pelo divisor de feixes $50:50$[15] (beam splitter $50:50$) e após a combinação esses feixes são medidos por fotodetectores.

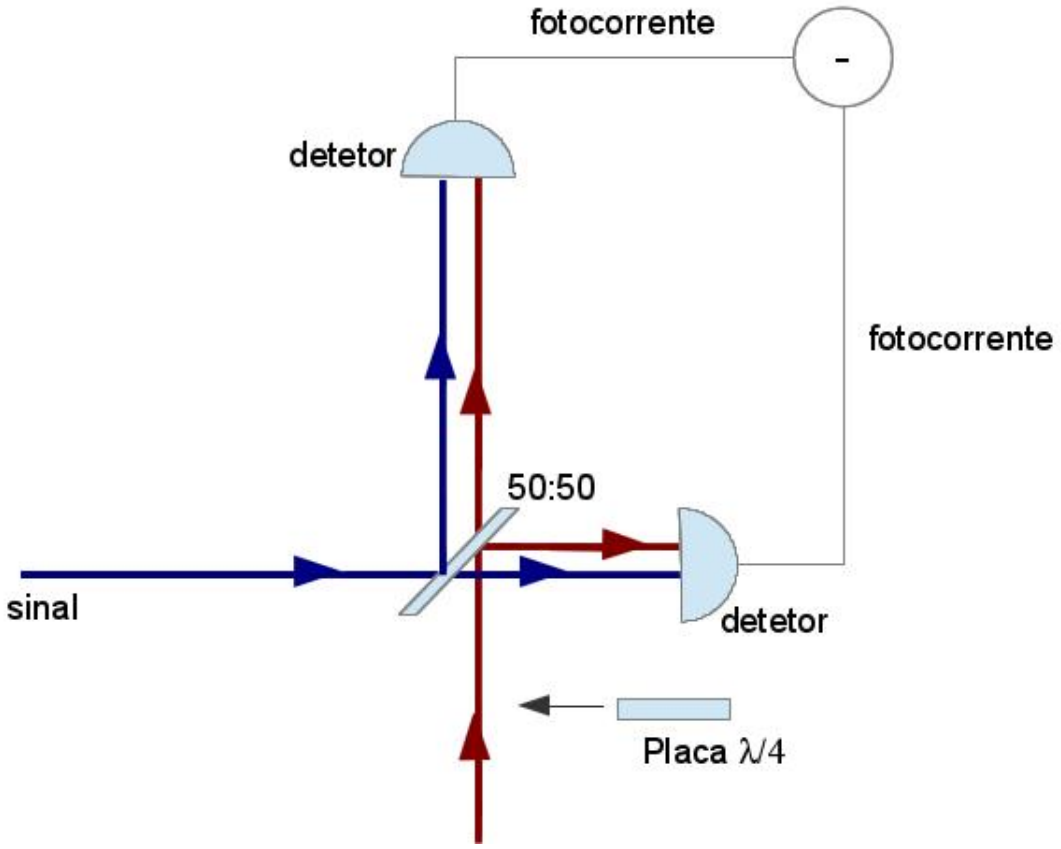


Figura 2.1: *Detecção homódina das quadraturas x e p, respectivamente. A diferença entre as duas fotocorrentes oriundas dos detetores é proporcional a x e, com a inserção de uma placa de quarto de onda, passa a ser proporcional a p.*

Um fotodetector mede o modo do campo eletromagnético "convertendo" fótons em elétrons, gerando assim uma corrente elétrica denominada fotocorrente $\hat{i}$. Podemos supor que a fotocorrente é proporcional ao número de fótons, $\hat{i} = q\hat{n} = q\hat{a}^{\dagger}\hat{a}$, onde q é uma constante (Braunstein and van Loock, 2005, pg.517). Os feixes de saída do divisor de feixes podem ser escrito como

$$\hat{a}_1 = \left(\hat{a}_{OL} + \hat{a}_S\right)/\sqrt{2}, \tag{2.83}$$

$$\hat{a}_2 = \left(\hat{a}_{OL} - \hat{a}_S\right)/\sqrt{2}, \tag{2.84}$$

onde $\hat{a}_{OL}$ é referente ao feixe do oscilador local e $\hat{a}_S$ é referente ao feixe do sinal. Devido ao fato de o feixe do oscilador local ser intenso, podemos reescrever o operador $\hat{a}_{OL}$ como

[15] A notação $50:50$ significa que a combinação é feita de maneira igual entre os dois feixes. O que significa usar um ângulo igual a $\pi/4$ na relação (2.81).

uma amplitude de campo complexa α_{OL} e com isso

$$\hat{a}_1 = (\alpha_{OL} + \hat{a}_S)/\sqrt{2}, \tag{2.85}$$
$$\hat{a}_2 = (\alpha_{OL} - \hat{a}_S)/\sqrt{2}. \tag{2.86}$$

Temos então que as fotocorrentes podem ser escritas como

$$\hat{i}_1 = q\hat{a}_1^\dagger \hat{a}_1 = q\left(\alpha_{OL}^* + \hat{a}_S^\dagger\right)(\alpha_{OL} + \hat{a}_S)/2, \tag{2.87}$$
$$\hat{i}_2 = q\hat{a}_2^\dagger \hat{a}_2 = q\left(\alpha_{OL}^* - \hat{a}_S^\dagger\right)(\alpha_{OL} - \hat{a}_S)/2. \tag{2.88}$$

A quantidade a ser medida agora será a diferença de fotocorrente. Logo,

$$\delta\hat{i} \equiv \hat{i}_1 - \hat{i}_2 = q(\alpha_{OL}^* \hat{a}_S + \alpha_{LO}\hat{a}_S^\dagger). \tag{2.89}$$

Lembrando que amplitude complexa α do oscilador local pode ser escrita como $\alpha_{OL} = |\alpha|e^{i\zeta}$ e não escrevendo mais os subíndices temos para $\zeta = 0$

$$\delta\hat{i} = q|\alpha|\left(\hat{a} + \hat{a}^\dagger\right) = 2q|\alpha|\hat{x}, \tag{2.90}$$

onde usamos a eq. (2.40). Com isso obtemos a quadratura $\hat{x}$ uma vez que $|\alpha|$ é conhecido. Ao escolhermos $\zeta = \pi/2$, o que equivale a usar uma placa de quarto de onda no oscilador local, obtemos o quadratura $\hat{p}$. Portanto, ajustando a fase do oscilador local podemos obter as quadraturas do campo e realizar até uma tomografia quântica do estado (Leonhardt, 1997, pg.84).

Nesse capítulo procuramos explicar boa parte da teoria necessária para uma descrição satisfatória dos sistemas a serem estudados nos capítulos seguintes. Obviamente, esse capítulo não tem por objetivo compilar todo o conhecimento em mecânica quântica e em teoria da informação. Detalhamos apenas os assuntos mais relevantes a essa Tese. Outros tópicos necessários para o bom entendimento dos assuntos específicos a cada um dos próximos capítulos serão discutidos quando se fizerem necessários.

Capítulo 3

Teletransporte quântico em variáveis contínuas

A extensão do protocolo de teletransporte quântico de variáveis discretas (vide capítulo 2, seção 2.4) para variáveis contínuas (dimensão do espaço de Hilbert infinita) foi um marco para a comunicação quântica (Braunstein and Kimble, 1998; Ralph and Lam, 1998; Vaidman, 1994). Conforme já vimos, o principal objetivo do teletransporte é garantir que ao final do protocolo o estado quântico que originalmente descrevia o sistema de Alice passe a descrever o sistema de Bob em outro local. Além disso, não há transmissão direta do sistema de Alice para Bob e nenhum conhecimento do estado de Alice é necessário para realizar o teletransporte. Essas duas propriedades ilustram claramente o porquê de o teletransporte ser uma ferramenta poderosa. De fato, para o teletransporte quântico ocorrer Alice e Bob só precisam ser capazes de agir localmente em seus sistemas, comunicar-se classicamente e compartilhar um canal quântico (estado emaranhado). No final do protocolo, o sistema de Alice não é mais descrito pelo seu estado original que agora descreve o sistema de Bob.

Em princípio, a execução perfeita do teletransporte ocorre apenas quando Alice e Bob compartilham um estado maximamente emaranhado. Por perfeita execução, queremos dizer que ao final do protocolo a probabilidade do sistema de Bob ser descrito pelo estado que originalmente descrevia o sistema de Alice é igual a um. Para sistemas descritos por variáveis discretas, e em particular qbits, tais estados maximamente emaranhados (estados de Bell) podem ser experimentalmente gerados em laboratório (Boschi et al., 1998; Bouwmeester et al., 1997). Para sistemas descritos por variáveis contínuas, a execução perfeita do protocolo requer um estado maximamente emaranhado (EPR), que não pode ser gerado em laboratório por exigir compressão infinita (Bowen, Treps, Buchler, Schnabel, Ralph, Bachor, Symul and Lam, 2003; Furusawa et al., 1998; Zhang et al., 2003).

Outra hipótese suposta, para um teletransporte perfeito, está relacionada com o conjunto de estados de entrada disponíveis para Alice, ou seja, os estados que

Alice pode teletransportar a Bob. Vamos considerar, por exemplo, o sistema descrito por variáveis discretas (capítulo 2, seção 2.4). Nesse caso supõe-se que o estado de entrada de Alice é dado por $|\phi\rangle = a|0\rangle + b|1\rangle$, onde a e b são números complexos arbitrários que satisfazem a condição de normalização $|a|^2+|b|^2 = 1$. Para o sistema de variáveis contínuas, em particular para estados coerentes $|\alpha\rangle$, com α complexo, é suposto que o conjunto de estados de Alice cobre todo o plano complexo (Braunstein et al., 2000; Braunstein and Kimble, 1998; Furusawa et al., 1998). Do ponto de vista teórico, quer para um qbit ou um estado coerente, esses pressupostos são adequados, a fim de determinar com rigor as condições que garantem um teletransporte "verdadeiramente" quântico, ou seja, as condições em que nenhum protocolo utilizando recursos puramente clássicos pode atingir a mesma eficiência prevista por protocolos com recursos quânticos (Braunstein et al., 2000). De um ponto de vista prático, esses pressupostos são válidos apenas para qbits, sendo irrealista para um sistema de variáveis contínuas. De fato, a energia de um estado coerente é proporcional a $|\alpha|^2$ e a fim de cobrir todo o plano complexo seria preciso estados com energia infinita. Além disso, quanto maior $|\alpha|$ menor a coerência quântica do estado (Ballentine, 1998, pg.573) e técnicas de transmissão direta do estado se tornam mais adequadas.

Com essas dois pressupostos mais realísticos em mente, ou seja, Alice e Bob compartilham um estado parcialmente emaranhado e o conjunto de estados de Alice são mais propensos a estar próximos a $|\alpha| = 0$, surge então uma pergunta. É possível melhorar a eficiência do protocolo de variáveis contínuas (PTVC) padrão, levando em conta esses dois fatos? Em outras palavras, ao abordar essas duas limitações de uma só vez não podemos transformar a desvantagem de um canal quântico dado por um estado emaranhado com compressão finita ($r < \infty$) em uma vantagem?

Para um conjunto de estados coerentes pertencentes a Alice, descritos por uma distribuição Gaussiana centrada no estado de vácuo (Braunstein et al., 2001) e quando Alice sempre teletransporta um único estado (Bowen, Treps, Buchler, Schnabel, Ralph, Symul and Lam, 2003; Ide et al., 2002; Mišta et al., 2010), a resposta a questão anterior é afirmativa. A modificação introduzida ao protocolo original em Braunstein et al. (2001) e Ide et al. (2002) foi deixar livre a escolha do ganho g (deslocamento nas quadraturas) feita por Bob ao fim do protocolo. Ajustando g apropriadamente, Bob pode maximizar a eficiência do teletransporte. Note que nas propostas anteriores Bob aplica esse ganho igualmente em ambas as quadraturas do seu estado (veja figura 3.1). No protocolo original (Braunstein and Kimble, 1998) temos $g = 1$, enquanto nas versões modificadas g foi ajustado em função dos estados de entrada e da compressão do canal de modo a aumentar a eficiência do PTVC. Uma estratégia idêntica foi empregada para melhorar a eficiência do *entanglement swapping* em variáveis contínuas (Polkinghorne and Ralph, 1999; van Loock and Braunstein, 1999), onde o g ótimo é ajustado para o estado especifico de entrada.

Com relação à distribuição de estados com Alice uma pergunta surge naturalmente: o que aconteceria se fossemos além de uma distribuição de probabilidade Gaussiana centrada no estado de vácuo e usarmos distribuições uniformes ou distribuições centradas em estados coerentes $|\beta\rangle$, $\beta \neq 0$? Mais importante, quais são as condições ideais para o PTVC ao introduzirmos mais do que um parâmetro livre na versão modificada (Mišta et al., 2010)? Nosso objetivo neste capítulo é investigar estas duas últimas perguntas em detalhes, e sem supor que sabemos o estado que será teletransportado (Bowen, Treps, Buchler, Schnabel, Ralph, Symul and Lam, 2003; Mišta et al., 2010). O único conhecimento que temos é a probabilidade de Alice escolher um estado coerente particular, $|\alpha\rangle$, de acordo com uma distribuição de probabilidade pré-definida.

Na seção 3.1 realizamos uma análise qualitativa e quantitativa do PTVC, inserindo pequenas modificações (parâmetros livres extras) no PTVC original. Com isso mostramos na subseção 3.2.1 que é possível conseguir aumentos significativos no desempenho adicionando parâmetros livres extras, os quais podem ser implementados por modificações mínimas no protocolo padrão. Além disso, na subseção 3.2.2 investigamos várias distribuições de probabilidade (ver figura 3.6) que descrevem os estados de entrada e mostramos as modificações ótimas para cada um delas. Modificações essas que sofrem apreciável alteração ao mudarmos a distribuição ou ao se deslocar no plano complexo essas distribuições centradas no estado de vácuo. E, como esperado, as mudanças no PTVC original não dependem apenas da distribuição de probabilidade específica associada ao estado de entrada de Alice, mas também do emaranhamento do canal.

3.1 Protocolo de teletransporte

Nessa seção procederemos com uma análise qualitativa do PTVC, dando ênfase às modificações que fizemos em relação ao PTVC original. Após essa análise, partiremos para a análise quantitativa, a fim de obter o estado de Bob após o fim protocolo.

3.1.1 Análise qualitativa

Antes de mergulhar nos detalhes matemáticos de nossos cálculos, vale a pena apresentar todo o quadro, ou seja, as escolhas que fizemos desde o início a fim de modificar a configuração original e a estratégia empregada para determinar o protocolo de teletransporte ótimo. Na proposta original (ver figura 3.1), um estado comprimido de dois modos com compressão r é compartilhado entre Alice e Bob. O modo 2 é dado a Alice e o modo 3 a Bob. O estado de Alice a ser teletransportado é representado pelo modo 1, que pode ser qualquer estado coerente $|\alpha\rangle$. Alice ao receber o estado a ser teletransportado (modo 1) o combina com o modo 2 através de um divisor de feixes $50:50$ (DF). Em seguida ela mede a posição e o momento (quadraturas do campo eletromagnético) dos modos u

e v, respectivamente, cujos resultados $\tilde{x}_u$ e $\tilde{p}_v$ são então comunicados a Bob de maneira clássica. Com essa informação Bob realiza deslocamentos na posição $(x_3 \to x_3 + g\tilde{x}_u)$ e no momento $(p_3 \to p_3 + g\tilde{p}_v)$ do modo 3. Tomando o ganho $g = \sqrt{2}$ para o caso no qual o canal esteja maximamente emaranhado ($r \to \infty$, o que é fisicamente impossível), o estado de Alice será perfeitamente teletransportado, ou seja, toda informação outrora contida no estado de Alice (modo 1) estará agora no estado de Bob (modo 3).

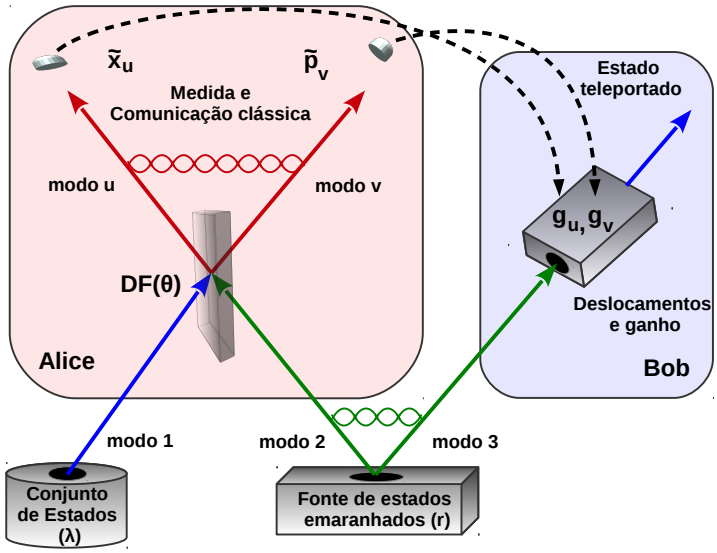


Figura 3.1: *Desenho esquemático do procedimento de teletransporte. Na proposta original (Braunstein and Kimble, 1998), os parâmetros do sistema eram dados por $\theta = \pi/4$ (50 : 50 DF), $g_u = g_v = g\sqrt{2}$, com $g = 1$, e o deslocamento na posição e momento dados por $x_3 \to x_3 + g_u\tilde{x}_u$ e $p_3 \to p_3 + g_v\tilde{p}_v$. Essas escolhas resultam em uma fidelidade média F_m independente da distribuição dos estados (rotulado por λ) de Alice. Aqui, fixaremos λ e a compressão r, e a otimização da fidelidade média F_m será implementada através dos três parâmetros livres, θ, g_v, e g_u, resultando em uma F_m que depende de r e λ. Veja o texto para maiores detalhes.*

A priori não há garantia de que uma escolha única para a transmitância do divisor de feixes ($\cos^2(\theta) = 1/2$), para os deslocamentos e para o ganho sejam ideais para todas as combinações de compressão finita r e de distribuição de probabilidade do conjunto de estados disponíveis para Alice. Portanto, a fim de procurar um protocolo ideal para um dado parâmetro de compressão r e distribuição de probabilidade, nós deixaremos o divisor de feixes com uma transmitância arbitrária ($DF(\theta)$), onde $0 < \theta < \pi/2$ (veja figura 3.1). Além disso, os deslocamentos das quadraturas e o ganho g implementados por Bob, após ser informado dos resultados das medidas de Alice ($\tilde{x}_u$ e $\tilde{p}_v$), também serão escolhidos de forma independente a fim de otimizar o protocolo. Formalmente, os deslocamentos de Bob são dados por $x_3 \to x_3 + g_u\tilde{x}_u$ e $p_3 \to p_3 + g_v\tilde{p}_v$, com g_u e g_v sendo escolhidos de modo a otimizar a eficiência do PTVC.

Nós empregaremos duas figuras de mérito para quantificar a otimização

do protocolo. Uma delas é realizada pelo cálculo da fidelidade média (capítulo 2, seção 2.5): Fixando-se a distribuição, escolhemos θ, g_v e g_u de modo a maximizar a fidelidade média. No entanto, como estamos trabalhando com uma média, pode haver estados com fidelidades inferiores àquela dada pelo protocolo original (Braunstein and Kimble, 1998). A outra figura de mérito corrige esse problema e podemos chamá-la de "nenhum estado é deixado para trás", ou de forma abreviada, condição NEDT. Esta condição é tal que os parâmetros ótimos θ, g_u e g_v são aqueles em que todos os estados de uma dada distribuição têm fidelidades maiores do que a prevista pelo PTVC original.

3.1.2 Análise quantitativa

No que se segue apresentamos os pormenores da análise matemática do PTVC modificado, no qual os três parâmetros θ, g_v e g_u são incorporados ao protocolo. Usamos indistintamente as palavras kets, estados e modos para nos referir ao mesmo objeto, ou seja, os modos do campo eletromagnético quantizado (veja capítulo 2, seção 2.6).

De acordo com o quarto postulado, podemos escrever o estado inicial do sistema antes do início do protocolo da seguinte forma

$$|\Psi\rangle = |\varphi\rangle \otimes |\Phi\rangle, \tag{3.1}$$

onde o estado $|\varphi\rangle$ é o estado que Alice deseja teletransportar (modo 1, veja figura 3.1) e o estado $|\Phi\rangle$ é o canal cujo modo 2 pertence a Alice e o modo 3 a Bob. Podemos reescrever esse estado na base da posição usando a equação (2.3),

$$|\Psi\rangle = \int_{-\infty}^{+\infty} dx_1 dx_2 dx_3 \varphi(x_1)\, \Phi(x_2, x_3)\, |x_1, x_2, x_3\rangle, \tag{3.2}$$

onde $\varphi(x_1) = \langle x_1|\varphi\rangle$, $\Phi(x_2, x_3) = \langle x_2, x_3|\Phi\rangle$, e o símbolo de integração indica integração sobre todas as variáveis. Salvo dito de outra forma, a ordenação dos estados será mantida da seguinte forma: $|$modo 1, modo 2, modo 3$\rangle$ (veja figura 3.1). O primeiro passo do protocolo consiste em enviar o modo 1 (estado de entrada) e o modo 2 (modo do canal que pertence a Alice) a um divisor de feixes (DF) com transmitância $\cos^2(\theta)$. A operação realizada pelo divisor de feixes é representada pela aplicação do operador (2.82). Logo, após a aplicação do operador o estado (3.2) pode ser escrito como

$$|\Psi'\rangle = \int dx_v dx_u dx_3 \varphi(x_v \sin(\theta) + x_u \cos(\theta))\, \Phi(x_v \cos(\theta) - x_u \sin(\theta), x_3)\, |x_v, x_u, x_3\rangle, \tag{3.3}$$

onde $x_v = x_1 \sin(\theta) + x_2 \cos(\theta)$ e $x_u = x_1 \cos(\theta) - x_2 \sin(\theta)$. Os limites inferior e superior da integral foram omitidos, a fim de tornar a notação menos carregada.

O próximo passo do protocolo consiste em medir a posição e momento dos modos u e v, respectivamente (veja figura 3.1). Para um campo eletromagnético quantizado, essa medida é feita por detecção homódina, onde as fotocorrentes atribuem números reais para as quadraturas $\hat{p}_v$ e $\hat{x}_u$ (veja capítulo 2, seção 2.6.3). Para medir o momento, Alice irá projetar o modo v na base do momento e dessa maneira é conveniente reescrever parte da equação (3.3) na base dos momentos. Para isso iremos fazer uso da relação (2.49). Deste modo a equação (3.3) pode ser escrita como

$$\begin{aligned} |\Psi'\rangle &= \frac{1}{\sqrt{\pi}} \int dp_v dx_v dx_u dx_3 \varphi\left(x_v \sin(\theta) + x_u \cos(\theta)\right) \Phi\left(x_v \cos(\theta) - x_u \sin(\theta), x_3\right) \\ &\quad \times e^{-2ix_v p_v} |p_v, x_u, x_3\rangle. \end{aligned} \tag{3.4}$$

No segundo passo do protocolo, Alice mede o momento do modo v e a posição do modo u (veja figura 3.1). Supondo que o resultado da medida seja $\tilde{p}_v$ e $\tilde{x}_u$, o estado total após o fim da medida é dado pela aplicação do terceiro postulado,

$$|\Psi''\rangle = \frac{\hat{P}_{\tilde{p}_v, \tilde{x}_u} |\Psi'\rangle}{\sqrt{\mathbb{P}(\tilde{p}_v, \tilde{x}_u)}}, \tag{3.5}$$

onde $\hat{P}_{\tilde{p}_v, \tilde{x}_u} = |\tilde{p}_v, \tilde{x}_u\rangle\langle\tilde{p}_v, \tilde{x}_u| \otimes \mathbb{1}_3$ é o projetor que descreve as medidas, com $\mathbb{1}_3$ sendo o operador identidade atuando sobre o modo 3, e $\mathbb{P}(\tilde{p}_v, \tilde{x}_u) = Tr(|\Psi'\rangle\langle\Psi'|\hat{P}_{\tilde{p}_v, \tilde{x}_u})$ é a probabilidade de medida do momento $\tilde{p}_v$ e da posição $\tilde{x}_u$ (ver capítulo 2 seção 2.1). Logo, o estado após a medição é dado por

$$|\Psi''\rangle = |\tilde{p}_v, \tilde{x}_u\rangle \otimes |\chi'\rangle, \tag{3.6}$$

onde o estado de Bob é

$$\begin{aligned} |\chi'\rangle &= \frac{1}{\sqrt{\pi \mathbb{P}\left(\hat{p}_v, \hat{x}_u\right)}} \int dx_v dx_3 \varphi\left(x_v \sin(\theta) + \tilde{x}_u \cos(\theta)\right) \Phi\left(x_v \cos(\theta) - \tilde{x}_u \sin(\theta), x_3\right) \\ &\quad \times e^{-2ix_v \tilde{p}_v} |x_3\rangle, \end{aligned} \tag{3.7}$$

com

$$\mathbb{P}\left(\tilde{p}_v, \tilde{x}_u\right) = \int dx_3 |\Psi'\left(\tilde{p}_v, \tilde{x}_u, x_3\right)|^2 \tag{3.8}$$

e

$$\begin{aligned} \Psi'\left(\tilde{p}_v, \tilde{x}_u, x_3\right) = \langle\tilde{p}_v, \tilde{x}_u, x_3|\Psi'\rangle &= \frac{1}{\sqrt{\pi}} \int dx_v \varphi\left(x_v \sin(\theta) + \tilde{x}_u \cos(\theta)\right) \\ &\quad \times \Phi\left(x_v \cos(\theta) - \tilde{x}_u \sin(\theta), x_3\right) e^{-2ix_v \hat{p}_v}. \end{aligned} \tag{3.9}$$

Para obter esses resultados a partir da equação (3.5) foram usadas as relações (2.47).

O terceiro passo do protocolo consiste em Alice enviar a Bob por um canal clássico os resultados de suas medições. Com essa informação Bob está apto a implementar o quarto e último passo do protocolo, o deslocamento das quadraturas do seu modo 3 seguindo a regra, $x_3 \rightarrow x_3 + g_u\tilde{x}_u$ e $p_3 \rightarrow p_3 + g_v\tilde{p}_v$. De uma maneira formal isto corresponde à aplicação do operador deslocamento $\hat{D}(\alpha)$ (veja capítulo 2, subseção 2.6.1), onde $\alpha = g_u\tilde{x}_u + ig_v\tilde{p}_v$. Assim, a aplicação desse operador resulta em

$$\hat{D}(g_u\tilde{x}_u + ig_v\tilde{p}_v)\,|x_3\rangle = e^{ig_ug_v\tilde{x}_u\tilde{p}_v}e^{2ig_v\tilde{p}_vx_3}|x_3 + g_u\tilde{x}_u\rangle. \tag{3.10}$$

Logo, realizando a mudança de variável $x_3 \rightarrow x_3 - g_u\tilde{x}_u$, o estado final de Bob, $|\chi\rangle = \hat{D}(g_u\tilde{x}_u + ig_v\tilde{p}_v)\,|\chi'\rangle$, pode ser escrito como

$$\begin{aligned}
|\chi\rangle &= \frac{e^{-ig_ug_v\tilde{x}_u\tilde{p}_v}}{\sqrt{\pi\mathbb{P}(\tilde{p}_v\tilde{x}_u)}}\int dx_v dx_3 \varphi(x_v\sin(\theta) + \tilde{x}_u\cos(\theta)) \\
&\quad \times\Phi(x_v\cos(\theta) - \tilde{x}_u\sin(\theta), x_3 - g_u\tilde{x}_u)\, e^{-2i(x_v - g_vx_3)\tilde{p}_v}|x_3\rangle \\
&= \int dx_3 \left(\frac{e^{-ig_ug_v\tilde{x}_u\tilde{p}_v}}{\sqrt{\pi\mathbb{P}(\tilde{p}_v\tilde{x}_u)}}\int dx_v \varphi(x_v\sin(\theta) + \tilde{x}_u\cos(\theta)) \right. \\
&\quad \left. \times\Phi(x_v\cos(\theta) - \tilde{x}_u\sin(\theta), x_3 - g_u\tilde{x}_u)\, e^{-2i(x_v - g_vx_3)\tilde{p}_v} \right)|x_3\rangle \\
&= \int dx_3 \chi(x_3)\,|x_3\rangle.
\end{aligned} \tag{3.11}$$

Note que $e^{-ig_ug_v\tilde{x}_u\tilde{p}_v}$ no estado acima é uma fase global irrelevante (veja capítulo 2) e pode ser suprimida. Vale a pena ressaltar que a equação (3.11), juntamente com as equações (3.8) e (3.9) são gerais. Elas nos permitem obter o estado teletransportado com Bob para qualquer estado de entrada e qualquer canal (estado emaranhado) compartilhado entre Alice e Bob. Caso o estado de entrada seja um estado coerente e o canal um estado de vácuo comprimido de dois modos, ao fixarmos os parâmetros do sistema em $g_v = g_u = \sqrt{2}$ e $\theta = \pi/4$, retornaremos no PTVC original.

3.2 Resultados

Após o termino do protocolo, devemos verificar o quão próximo o estado de Bob se encontra do estado de entrada originalmente com Alice. Isso é feito por meio de uma medida de distância entre dois estados quânticos denominada fidelidade (veja, capítulo 2, seção 2.5).

3.2.1 Análise da fidelidade

Para realizar a análise da eficiência do teletransporte faremos uso da fidelidade, eq. (2.37), usando como estados de entrada estados coerentes, eq. (2.65), e como

canal um estado de vácuo comprimido de dois modos, eq. (2.28), de modo que a fidelidade pode ser escrita como

$$F\left(|\alpha\rangle,\hat{\rho}_{out}\right)=\frac{\exp\left[-\frac{f_1(\theta,g_v)}{f_2(\theta,g_v)}Im\left[\alpha\right]^2-\frac{f_1\left(\theta+\frac{\pi}{2},g_u\right)}{f_2\left(\theta-\frac{\pi}{2},g_u\right)}Re\left[\alpha\right]^2\right]}{\sqrt{f_2\left(\theta,g_v\right)f_2\left(\theta-\frac{\pi}{2},g_u\right)}}, \tag{3.12}$$

onde

$$\begin{aligned} f_1\left(\theta,g_v\right) &= \left(1-g_v\sin\left(\theta\right)\right)^2, & (3.13)\\ f_2\left(\theta,g_v\right) &= \left[\left(2+g_v^2\right)\cosh^2\left(r\right)+g_v^2\cos\left(2\theta\right)\sinh^2\left(r\right)\right. \\ &\quad \left.-2g_v\cos\left(\theta\right)\sinh\left(2r\right)\right]/2. & (3.14)\end{aligned}$$

A equação (3.12), depende dos parâmetros livres θ, g_v, g_u e do estado $|\alpha\rangle$. Para que a fidelidade fique independente do estado devemos ter $f_1\left(\theta,g_v\right)=f_1\left(\theta+\pi/2,g_u\right)=0$. A solução que satisfaz essa equação é dada por $g_v=\csc\left(\theta\right)$ e $g_u=\sec\left(\theta\right)$. Retornando esses valores na equação (3.12) e maximizando-a em relação a θ, obtemos $\theta=\pi/4$ e consequentemente $g_v=g_u=\sqrt{2}$ como parâmetros ótimos, de modo que a fidelidade ótima para essa configuração será $F(|\alpha\rangle,\hat{\rho}_{out})=1/(1+e^{-2r})$. Essa configuração de parâmetros e essa fidelidade são as mesmas do PTVC original (Braunstein and Kimble, 1998). No entanto, a maximização não é feita levando em conta qual estado coerente e teletransportado $|\alpha\rangle$, ou em qual região do plano ele se encontra ou a relação do teletransporte com os parâmetros de interação (θ, g_v, g_u) . O que faremos a seguir é realizar duas modificações simples no protocolo original e analisar suas consequências ao supor que conhecemos $|\alpha\rangle$.

A primeira modificação consiste em assumir que $g_v=g_u=g$, com g escolhido de tal forma a se obter a melhor fidelidade possível (Braunstein et al., 2001; Ide et al., 2002; van Loock and Braunstein, 1999), mantendo a transmitância do divisor de feixes usada no PTVC original. Obviamente a fidelidade maximizada ficará em função do estado $|\alpha\rangle$ e nosso intuito é verificar se há um estado (ou conjunto de estados) onde o ganho na fidelidade é significativo em relação a PTVC original, para um parâmetro g escolhido. Nessa mesma linha aplicaremos nossa segunda modificação, que consiste em maximizar a fidelidade, eq. (3.12), em função dos três parâmetros livres , g_v, g_u e θ.

Implementando a primeira estratégia, ou seja, fixando-se a transmitância do DF em $\cos(\theta)=1/2$ e $g_v=g_u=g$, calculamos a fidelidade ótima $F(|\alpha\rangle,\hat{\rho}_{out})$ supondo $r=0.5$. Os resultados são mostrados na figura 3.2, onde o gráfico da esquerda mostra a fidelidade ótima e o da direita a parâmetro g ótimo. Claramente podemos ver que a fidelidade ótima e o parâmetro g ótimo possuem uma simetria radial, o que significa que todo estado coerente com a mesma amplitude $|\alpha|$ possui a mesma fidelidade ótima com o mesmo g. Além disso a fidelidade tem seu valor máximo, $F\left(|\alpha\rangle,\hat{\rho}_{out}\right)=1$, no estado de vácuo. Quando nos afastamos do estado de vácuo, ou seja, aumentamos $|\alpha|$, a fidelidade

ótima e o parâmetro g ótimo tendem aos valores do PTVC original.

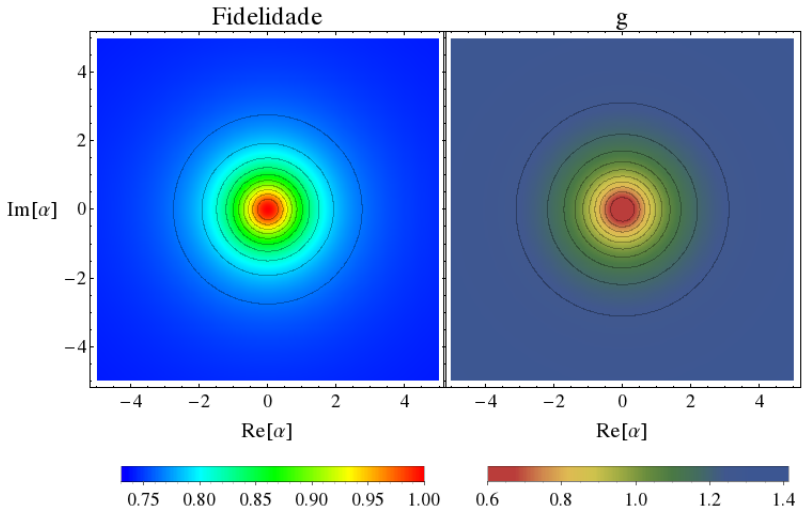


Figura 3.2: *Esquerda: Fidelidade $F(|\alpha\rangle)$ em função dos valores reais e imaginários do estado coerente $|\alpha\rangle$, com $\theta = \pi/4$, $r = 0.5$, e o parâmetro livre $g_v = g_u = g$ escolhido de tal forma a otimizar a fidelidade para cada $|\alpha\rangle$. Direita: g em função dos valores reais e imaginários do estado coerente, que levam à fidelidade ótima do gráfico à esquerda.*

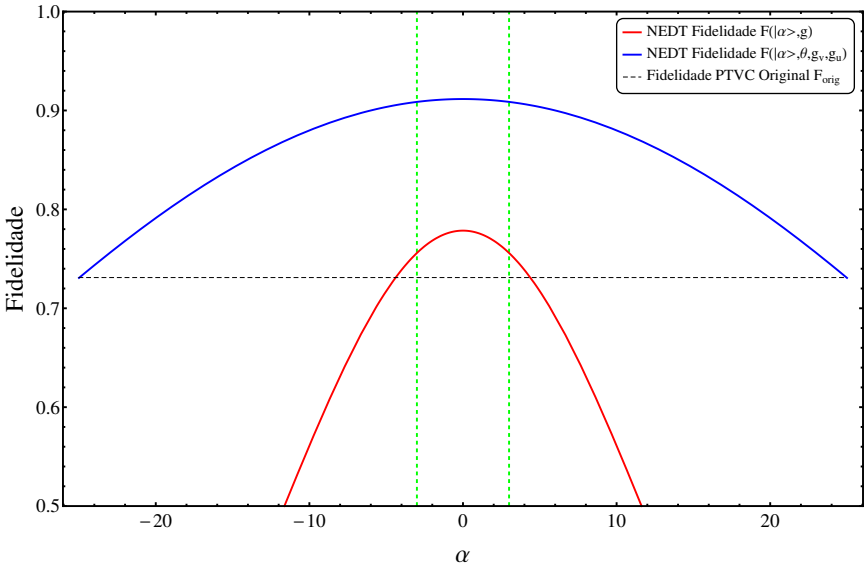


Figura 3.3: *No que se segue todas as fidelidades foram calculadas supondo um parâmetro de compressão $r = 0.5$ para o canal. A curva inferior vermelha/sólida dá a fidelidade em função de $|\alpha|$ para $\theta = \pi/4$ e $g_v = g_u = g$, onde g é o parâmetro que leva à fidelidade ótima para estados na borda do círculo de raio $|\alpha| = 3$, delimitado pelas retas verticais. A curva superior azul/sólida é a fidelidade para os estados $|\alpha\rangle$ que se encontram tanto sobre os eixos real ou imaginário. O trio de parâmetros θ, g_v, e g_u são fixos e agora escolhidos de modo a dar a fidelidade ótima para os estados nos pontos extremos da reta real/imaginária centrada na origem e com comprimento $2|\alpha|$, com $|\alpha| = 3$. Podemos observar que para a segunda estratégia (curva superior azul/sólida) as fidelidades para todos os estados dentro das linhas reais/imaginarias são sempre maiores do que os previstos pelo PTVC original (curva preta segmentada) e das dadas pela primeira estratégia (curva vermelha/sólida).*

Um ponto interessante que devemos mencionar é que ao fixarmos $\theta = \pi/4$ e $g_v = g_u = g$ e maximizarmos a fidelidade para um estado, todos os estados dentro de um círculo de raio igual ao módulo desse estado terão fidelidades maiores ou iguais à fidelidade do PTVC original. Isso ilustra perfeitamente a figura de mérito mencionada anteriormente: "nenhum estado é deixado para trás" (NEDT). A figura 3.3 mostra a condição NEDT, onde maximizamos a fidelidade para o estado $|\alpha| = 3$ (linhas verdes tracejadas) e usamos o parâmetro g dessa maximização para calcular a fidelidade de todos os estados sobre a reta real (curva vermelha). Vemos que para todos os estados dentro do círculo de raio $|\alpha| = 3$ (retas verdes tracejadas) a fidelidade é maior que a fidelidade do PTVC original (reta preta tracejada). Realizamos o cálculo para os estados sobre a reta real, $Im[\alpha] = 0$, mas o cálculo pode ser feito para qualquer estado dentro do círculo, mostrando que a condição NEDT é respeitada.

Podemos agora analisar nossa segunda estratégia, ou seja, vamos deixar os parâmetros g_v, g_u e θ serem escolhidos de forma independente, de modo a maximizar a fidelidade. Devido a dificuldade de se realizar a maximização de forma analítica, devemos então utilizar métodos numéricos para realizar a maximização. O resultado dessa maximização é mostrado na figura 3.4, com a fidelidade ótima $F(|\alpha\rangle, \hat{\rho}_{out})$ (representada na figura por $\mathcal{F}$) como uma função de $|\alpha\rangle$. Os parâmetros θ, g_v e g_u que maximizam essa fidelidade são mostrados na figura 3.5, também como função de $|\alpha\rangle$.

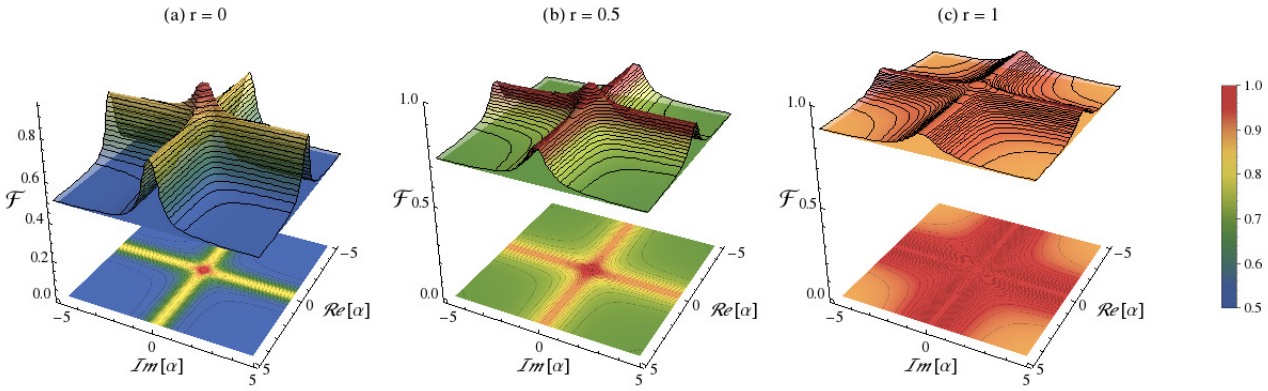


Figura 3.4: *Os gráficos mostram a fidelidade ótima $F(|\alpha\rangle)$ em função das partes real e imaginária do estado coerente $|\alpha\rangle$ para canais com compressão (a) $r = 0$, (b) $r = 0.5$, e (c) $r = 1$ (da esquerda para a direita). Os parâmetros g_v, g_u, e θ são escolhidos de forma a otimizar $F(|\alpha\rangle)$ para cada estado $|\alpha\rangle$. Mostramos a fidelidade ótima, $F(|\alpha\rangle)$, em gráficos 3D (em cima) com seus respectivos gráficos de densidade (em baixo). Os planos logo abaixo dos gráficos em 3D são da fidelidade prevista pelo PTVC original.*

A primeira coisa que notamos é a perda da simetria radial quando os parâmetros são modificados independentemente no cálculo da fidelidade ótima. Além disso, podemos observar que para os estados ao longo do eixo real e imaginário temos um aumento muito significativo na fidelidade do estado teletransportado. Ao nos movermos para e sobre os eixos diagonais a fidelidade ótima tende ao valores dado pelo PTVC

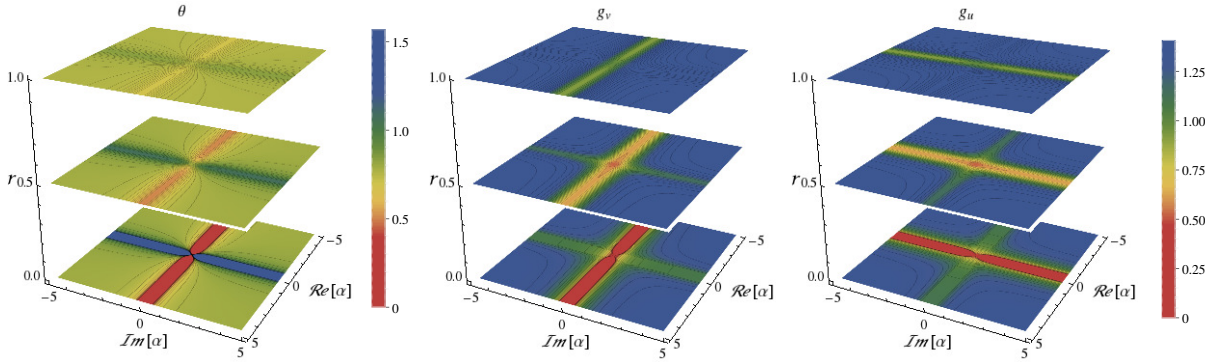


Figura 3.5: *Da esquerda para a direta temos os gráficos de densidade dos parâmetros ótimos θ, g_v, e g_u resultando nas fidelidades ótimas mostradas na figura 3.4. O eixo z representa o parâmetro de compressão r, que aumenta de baixo para cima ($r = 0, 0.5,$ e 1.0).*

original. Isso não acontece, porém, nos eixos real e imaginário. Para estados sobre esses eixos, ao nos afastarmos do estado de vácuo a fidelidade ótima se estabiliza em um valor acima da fidelidade do PTVC original. A medida que aumentamos r todos os valores da fidelidade ótima, incluindo a dos estados sobre os eixos real e imaginário, tendem ao valores da fidelidade do PTVC original (figura 3.4 (c)). Esse comportamento também é visto para os parâmetros θ, g_v e g_u. Ao aumentarmos r esses parâmetros tendem aos parâmetros usados no PTVC original.

3.2.2 Análise da fidelidade média

Vamos agora estudar o caso em que Alice possui um conjunto de estados coerentes, eq. (2.65). O canal compartilhado por Bob e Alice continua sendo um estado de vácuo comprimido de dois modos, eq. (2.28). Iremos trabalhar com várias distribuições de probabilidade diferentes, $P(|\alpha\rangle)$, para o conjunto de estados de Alice, cuja condição de normalização é dada por

$$\begin{aligned} \int P\left(|\alpha\rangle\right) d|\alpha\rangle &\equiv \int_{-\infty}^{+\infty}\int_{-\infty}^{+\infty} P\left(\alpha\right) dRe\left[\alpha\right] dIm\left[\alpha\right] \\ &\equiv \int_{0}^{2\pi}\int_{0}^{+\infty} P\left(\alpha\right)|\alpha| d|\alpha| d\omega = 1, \end{aligned} \tag{3.15}$$

onde $\alpha = Re[\alpha] + iIm[\alpha] = |\alpha|e^{i\omega}$. Uma representação pictórica das várias distribuições $P(\alpha)$ que trataremos pode ser vista na figura 3.6.

Estados puramente reais ou imaginários

As duas primeiras distribuições estudadas confinam os estados $|\alpha\rangle$ aos eixos real ou imaginário. Nós supomos que os estados estão distribuídos uniformemente ao longo do eixo real ou imaginário de $-R$ a R, onde $R > 0$.

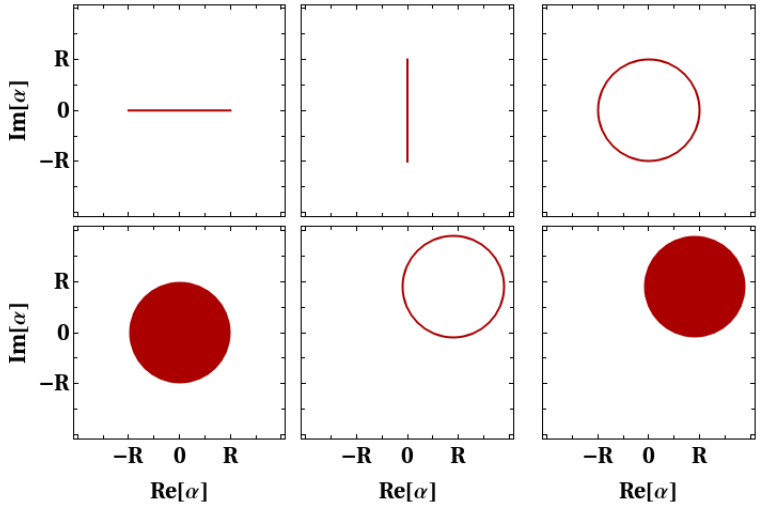


Figura 3.6: *Representação esquemática de distribuições de probabilidade uniforme $P(\alpha)$ para os estados de entrada de Alice. Em cima, da esquerda para a direita : estados coerentes $|\alpha\rangle$ com apenas a parte real , apenas com a parte imaginária, e estados distribuídos em uma circunferência. Em baixo, da esquerda para a direita: Estados distribuídos em um disco e estados distribuídos em uma circunferência e em um disco centrados em um estado $|\beta\rangle$, $\beta \neq 0$.*

A distribuição para α real é dada por

$$P_r(\alpha) = \delta\left(Im\left[\alpha\right]\right)\Theta\left(R^2 - Re\left[\alpha\right]^2\right)/2R, \tag{3.16}$$

com $\delta(x)$ sendo a função delta de Dirac e $\Theta(x)$ a função Θ de Heaviside ($\Theta(x) = 0$ se $x < 0$ e $\Theta(x) = 1$ para $x \geq 0$). A distribuição para α imaginário é dada por

$$P_i(\alpha) = \delta(Re[\alpha])\Theta(R^2 - Im[\alpha]^2)/2R. \tag{3.17}$$

Inserindo as eqs. (3.12) e (3.16) na eq. (2.38) obtemos a fidelidade média dos estados distribuídos na reta real,

$$F_m^{real} = \frac{\sqrt{\pi}}{2R}\frac{\mathrm{Erf}\left[R\sqrt{\frac{f_1(\theta+\pi/2,g_u)}{f_2(\theta-\pi/2,g_u)}}\right]}{\left[f_1(\theta+\pi/2,g_u)f_2(\theta,g_v)\right]^{1/2}}, \tag{3.18}$$

onde $\mathrm{Erf}[x] = \frac{2}{\sqrt{\pi}}\int_0^x e^{-t^2}dt$ é a função erro.

Uma vez que a dependência de g_v na eq. (3.18) é dada apenas por $f_2(\theta, g_v)^{1/2}$, podemos realizar a maximização da fidelidade média em função de g_v de forma analítica,

$$g_v^{ot} = \frac{\sinh\left(2r\right)\cos\left(\theta^{ot}\right)}{\cosh\left(r\right) + \cos\left(2\theta^{ot}\right)\sinh^2\left(r\right)}, \tag{3.19}$$

onde g_v^{ot} e θ^{ot} são os parâmetros ótimos que maximizam a fidelidade média. Ao substituirmos a eq. (3.19) na eq. (3.18) irão restar dois parâmetros para maximizarmos, θ e

g_u. Porém, devido à presença da função erro na eq. (3.18), não conseguimos uma solução analítica para esses parâmetros. Assim, teremos que obter soluções numéricas uma vez especificados o parâmetro de compressão r e o intervalo da distribuição R.

Repetindo os mesmo cálculos para uma distribuição uniforme de estados na reta imaginária, que varia entre $-R$ a R, temos

$$F_m^{imag} = \frac{\sqrt{\pi}}{2R} \frac{\mathrm{Erf}\left[R\sqrt{\frac{f_1(\theta,g_v)}{f_2(\theta,g_v)}}\right]}{[f_1(\theta,g_v)f_2(\theta-\pi/2,g_u)]^{1/2}}. \tag{3.20}$$

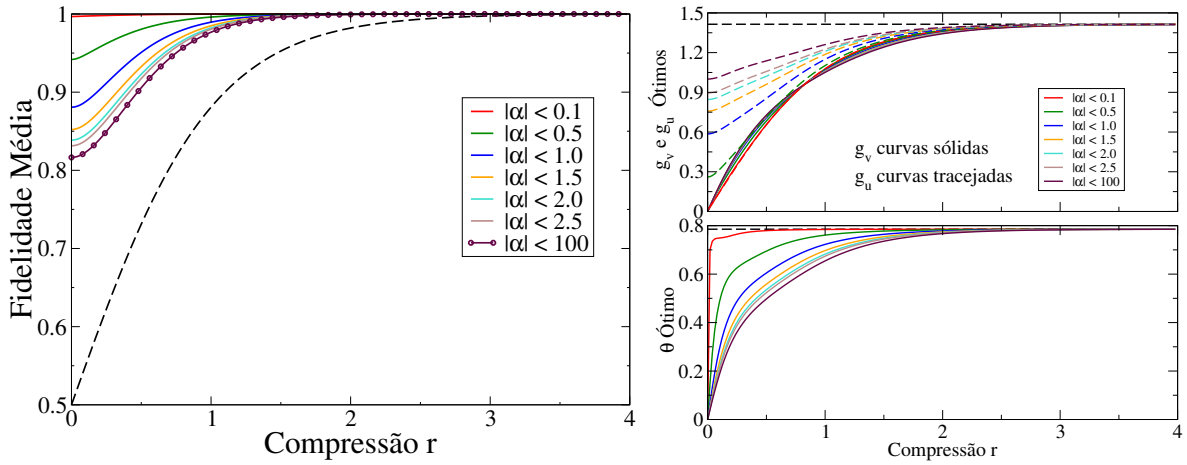
Os papeis de g_u e g_v agora são invertidos, de modo que a dependência de g_u na eq. (3.20) é dada apenas pela equação $f_2(\theta-\pi/2,g_u)^{1/2}$. Devido a isso a obtenção da solução analítica é possível,

$$g_u^{ot} = \frac{\sinh(2r)\sin\theta^{ot}}{\cosh^2(r) - \cos(2\theta^{ot})\sinh^2(r)}, \tag{3.21}$$

onde g_u^{ot} e θ^{ot} são os parâmetros ótimos que maximizam a fidelidade média. Como no caso da reta real, não é possível obter soluções analíticas para os outros dois parâmetros, θ e g_v, devido à presença da função erro. Portanto, para resolver completamente o problema de maximização fazemos uso de métodos numéricos uma vez especificados o parâmetro de compressão r e o intervalo da distribuição R.

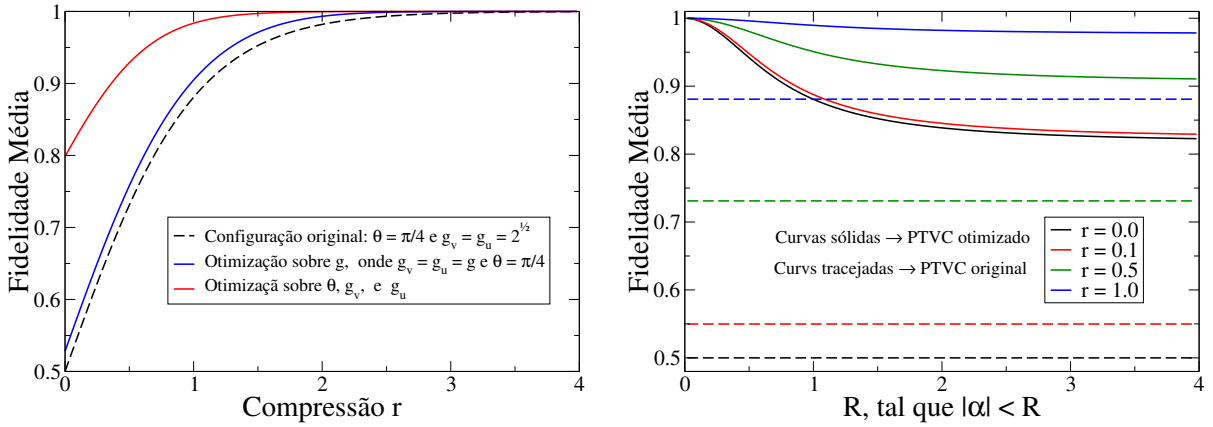
A figura (3.7(a)) mostra a fidelidade ótima F_m^{real} e F_m^{imag} para várias distribuições com $|\alpha| \leq R$ como uma função do parâmetro de compressão r do canal. A primeira coisa que notamos é que as fidelidades médias ótimas (maximizadas) são as mesmas para as distribuições real e imaginária. A segunda coisa a se destacar é que quanto menor o intervalo da distribuição maior a eficiência do teletransporte. Isto é esperado já que ao se diminuir o intervalo os estados disponíveis para Alice se tornam cada vez mais similares. Ao incrementarmos o intervalo R a fidelidade média ótima tende a um limite assintótico (curva com círculos marrons na figura 3.7(a)) e possui um valor muito superior à fidelidade média dada pelo PTVC original (curva tracejada na figura (3.7(a))). A figura 3.7(b) mostra os parâmetros ótimos θ, g_v, e g_u usados para o cálculo da fidelidade ótima na figura (3.7(a)).

Nós também realizamos a comparação de quanto ganhamos em eficiência otimizando a fidelidade média, considerando os três parâmetros livres θ, g_v e g_u, contra a otimização da fidelidade média considerando $\theta = \pi/4$ e $g_v = g_u = g$ onde apenas g (o ganho) é livre (Braunstein et al., 2001; Ide et al., 2002; van Loock and Braunstein, 1999). Como podemos ver na figura 3.8(a), obtemos um ganho considerável em eficiência quando permitimos que os três parâmetros sejam livremente ajustados para a essa distribuição, quando comparado com o cenário de um único parâmetro. Além disso, verificamos que quanto maior R menor a eficiência da otimização considerando um único parâmetro. Para



(a) (b)

Figura 3.7: *(a)As curvas sólidas dão a fidelidade média ótima (maximizada) como função do canal emaranhado (parâmetro de compressão r) para as distribuições uniformes real e imaginária, cujos intervalos R aumentam de cima para baixo. Curva tracejada: fidelidade média dada pelo PTVC original, que não depende de nenhuma distribuição em especial. Nota-se que as fidelidades médias ótimas coincidem para as distribuições reais e imaginárias e que obtemos ganhos expressivos em eficiência com canais que possuem baixo grau de emaranhamento.(b) Parâmetros usados no cálculo da fidelidade média ótima mostrada na figura 3.7(a) para estados que se encontram sobre a reta real. Note que há muitas curvas para g_v^{ot} que estão muito próximas umas das outras. Para g_u^{ot} o intervalo R aumenta de baixo para cima, enquanto para θ aumenta de cima para baixo. As curvas pretas tracejadas indicam os valores utilizados no PTVC original ($g_v = g_u = \sqrt{2} \approx 1.41$ e $\theta = \pi/4 \approx 0.79$). Para a distribuição imaginária, $g_v \leftrightarrow g_u$ e $\theta \to \pi/2 - \theta$ nos gráficos acima.*



(a) (b)

Figura 3.8: *(a)As curvas acima foram calculadas considerando tanto uma distribuição uniforme real ou imaginária com $|\alpha| \leq R = 5.0$. É evidente a partir da figura que, a fim de obter um ganho expressivo em termos de eficiência para os canais quânticos com baixo grau de emaranhamento é fundamental ao se otimizar a fidelidade média fazer uso dos três parâmetros livres. (b) As curvas acima denotam a fidelidade média ótima como uma função do intervalo R da distribuição. Essas curvas são as mesmas para as distribuições reais e imaginárias e o parâmetro de compressão r aumenta de baixo para cima.*

um R não muito grande, temos que recorrer à otimização com três parâmetros para obter ganhos de eficiência bem acima do protocolo original.

Na figura 3.8(b) mostramos a fidelidade média ótima em função do intervalo R de uma distribuição uniforme que descreve o conjunto de estados de entrada de Alice. É evidente a partir dos dados que, para todas as faixas de R, temos um melhor desempenho com o PTVC otimizado com três parâmetros e que quanto menor o grau de emaranhamento do canal maiores os ganhos em eficiência.

Estados distribuídos em um disco ou em uma circunferência

Para um conjunto de estados $|\alpha\rangle$ disponíveis a Alice possuindo a mesma amplitude $|\alpha| = R$ e fases ω dada por uma distribuição uniforme, onde $0 \leq \omega < 2\pi$, temos na representação do plano complexo $|\alpha\rangle$ uma circunferência de raio R centrada no vácuo (Veja figura 3.6). Assim, podemos escrever a distribuição de probabilidade como

$$P_c(\alpha) = \delta\left(|\alpha| - R\right) / \left(2\pi R\right). \tag{3.22}$$

Inserindo a eq. (3.22) na eq. (2.38) temos a fidelidade média para estados uniformemente distribuídos em uma circunferência de raio R da seguinte forma,

$$F_m^c = \frac{e^{-h_+(\theta,g_v,g_u)R^2} I_0[h_-(\theta,g_v,g_u)R^2]}{\sqrt{f_2(\theta,g_v)f_2(\theta-\pi/2,g_u)}}, \tag{3.23}$$

onde

$$h_\pm(\theta,g_v,g_u) = \left(\frac{f_1(\theta+\pi/2,g_u)}{2f_2(\theta-\pi/2,g_u)} \pm \frac{f_1(\theta,g_v)}{2f_2(\theta,g_v)}\right) \tag{3.24}$$

e $I_0[x]$ é a função de Bessel modificada de primeiro tipo, ou seja, solução de $x^2 I_n[x]'' + xI_n[x]' - (x^2+n^2)I_n[x] = 0$ com $n = 0$ e condições de contorno $I_0[0] = 1$ e $\lim_{x\to\pm\infty} I_0[x] \to \infty$.

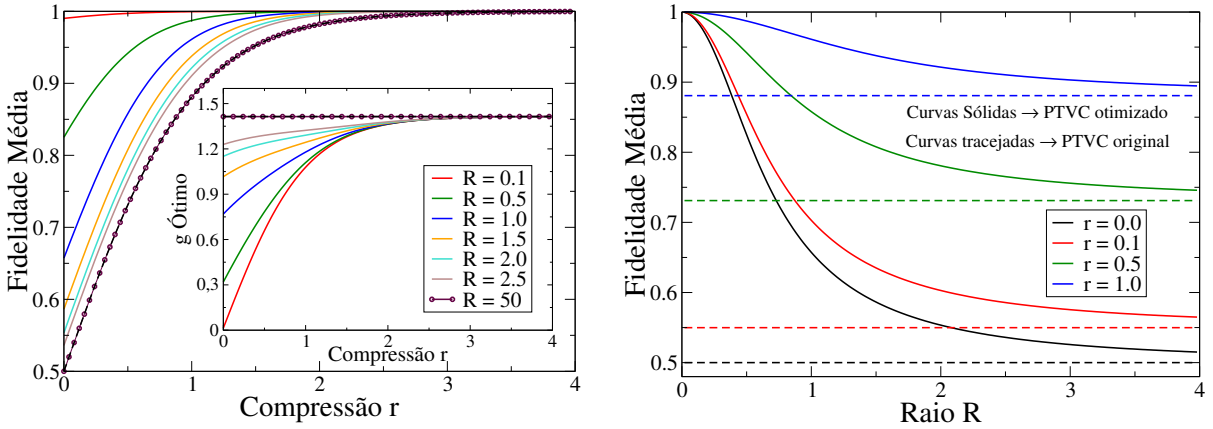
A existência da função de Bessel torna a solução analítica do problema de otimização inviável. No entanto, verificamos numericamente para diversas combinações aleatórias de r e R que o conjunto de parâmetros θ, g_v e g_u que leva à fidelidade média ótima para essa distribuição é dado por $\theta = \pi/4$ e $g_v = g_u = g$. Portanto, inserindo os parâmetros anteriores na eq. (3.23), podemos reformular a determinação da fidelidade média ótima para o problema de otimização de um única variável. Logo, a fidelidade média pode ser escrita como

$$F_m^c = \frac{2\exp\left[-\frac{\left(\sqrt{2}g-2\right)^2 R^2 \operatorname{sech} r}{2(g^2+2)\cosh(r)-4\sqrt{2}g\sinh(r)}\right]}{(g^2+2)\cosh^2(r) - \sqrt{2}g\sinh(2r)}, \tag{3.25}$$

onde a fidelidade média ótima é dada maximizando a equação acima em função de g. Ao realizar o procedimento de maximização o parâmetro ótimo g é dado pela equação cúbica

$$\sqrt{2}(e^r \sinh(2r)\cosh r + 2R^2) - ge^r(3\cosh(2r) - 1)\cosh r - g^2\sqrt{2}(R^2 - 3e^r \sinh r \cosh^2 r) - g^3 e^r \cosh^3 r = 0.$$

A figura 3.9(a) mostra a fidelidade ótima F_m^c para várias distribuições uniformes com estados distribuídos ao longo da circunferência de raio R em função do emaranhamento do canal r. Na figura 3.9(b) mostramos a fidelidade média ótima F_m^c em função do raio R para valores fixos do emaranhamento do canal.



(a) (b)

Figura 3.9: *(a) Curvas sólidas são as fidelidades médias em função do emaranhamento do canal (compressão r) para estados uniformemente distribuídos em um círculo de raio R, com R aumentando de cima para baixo. Gráfico interno: Ganho otimizado $g_v = g_u = g$ resultando nas fidelidades médias ótimas mostradas no gráfico principal. Aqui, R aumenta de baixo para cima. Curvas tracejadas: fidelidade média (gráfico principal), que não depende de nenhuma distribuição específica, e g (gráfico interno) de acordo com o PTVC original. As curvas tracejadas são indistinguíveis das curva com $R = 50$. (b) Esses gráficos mostram a fidelidade média ótima em função do raio R da circunferência, com o parâmetro de compressão r crescente de baixo para cima.*

Olhando a figura 3.9(a), podemos ver que, quanto menor o raio R da distribuição maior a eficiência. Além disso, para $R = 0$ temos $F_m^c = 1$ para qualquer valor do parâmetro de compressão, o que era esperado já que possuímos apenas um estado para teletransportar, o estado de vácuo. A medida que aumentamos R a fidelidade média ótima diminui, e ao contrário das distribuições reais e imaginárias ela não tende a um limite assimptótico superior ao dado pelo PTVC original (curva círculos/marrons na figura 3.9(a)). Na verdade, F_m^c se aproxima da fidelidade do PTVC original ao se aumentar R (curva tracejada na figura 3.9(a)).

Supondo agora que a amplitude e a fase são dados por distribuições uniformes independentes, ou seja, os estados de entrada estão contidos em um disco de raio R

($|\alpha| \leq R$ e $0 \leq \omega < 2\pi$), temos então

$$P_d(\alpha) = \Theta(R - |\alpha|) / (\pi R^2). \tag{3.26}$$

Inserindo a eq. (3.26) na eq. (2.38) temos

$$F_m^d = \frac{2}{R^2} \int_0^R R' F_m^c(R')\, dR', \tag{3.27}$$

com $F_m^c(R')$ sendo dada pela eq. (3.23) como uma função do raio R'. A última integração na eq. (3.27) não pode ser calculada analiticamente e devemos trabalhar numericamente a fim de obter a fidelidade média ótima.

Realizamos um estudo numérico sistemático para vários valores do parâmetro de compressão r e raios R da distribuição em forma de disco, obtendo em todos os casos os parâmetros ótimos $\theta^{ot} = \pi/4$ e $g_v = g_u = g$. De modo que, substituindo esses parâmetros na eq. (3.27), a última integração pode ser calculada resultando então na fidelidade média dada por

$$F_m^d = \frac{2\left(1 - \exp\left[\frac{-\left(\sqrt{2}-g\right)^2 R^2}{(2+g^2)\cosh^2(r) - \sqrt{2}g\sinh(2r)}\right]\right)}{\left(\sqrt{2}-g\right)^2 R^2}. \tag{3.28}$$

A fidelidade média ótima é obtida maximizando a equação acima em relação a g. Essa maximização resulta em uma equação transcendental, demasiadamente grande de modo que não será escrita aqui. No entanto, uma vez que temos um problema de maximização de um parâmetro, a sua solução numérica é trivialmente obtida por métodos convencionais e podemos facilmente calcular a fidelidade média ótima para uma distribuição de estados em forma de disco, quando r e R são especificados.

As figuras 3.10(a) e 3.10(b) mostram, respectivamente, a fidelidade média ótima em função do emaranhamento do canal (parâmetro de compressão r) e em função do raio R do disco, sobre o qual os estados de entrada estão uniformemente distribuídos. Elas possuem as mesmas características qualitativas já explicadas para a distribuição de estados em uma circunferência. Quantitativamente no entanto, a fidelidade média tem um melhor desempenho para um dado disco de raio R quando comparada com uma circunferência com o mesmo raio. Isto é compreendido observando que o disco nada mais é do que a união de todas as circunferências de raio inferior e igual a R. E, uma vez que demostramos que o menor R tem uma maior fidelidade em uma distribuição dada por um circunferência, fica claro que a fidelidade média ótima de um disco deve superar a fidelidade ótima para um circunferência de mesmo raio R.

Se queremos trabalhar com estados distribuídos em uma circunferência ou disco centrado em um estado $|\beta\rangle$, podemos simplesmente substituir α por $\alpha - \beta$ no lado

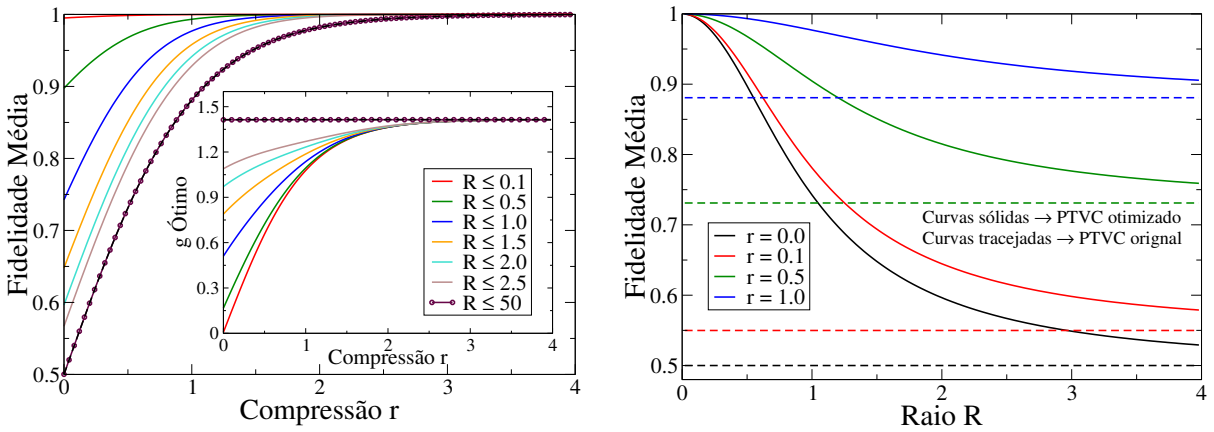


Figura 3.10: *(a) As curvas sólidas são a fidelidade média em função do emaranhamento do canal (compressão r) para estado uniformemente distribuídos em um disco de raio R, onde R aumenta de cima para baixo. Curvas tracejadas: fidelidade média dada pelo PTVC original. Gráfico interno: O ganho otimizado $g_v = g_u = g$ que resulta nas fidelidades mostradas no gráfico principal. Aqui, R aumenta de baixo para cima e a curva tracejada é g de acordo com o PTVC original. O θ ótimo é sempre dado por $\pi/4$. Note que a curva tracejada é indistinguível a partir de $R \approx 50$. (b) As curvas mostram a fidelidade média ótima em função do raio R do disco, com o parâmetro de compressão r aumentando de baixo para cima.*

direito das equações (3.22) e (3.26). As expressões para as fidelidades média ótimas não podem ser colocadas de uma forma analítica simples para um β arbitrário e devemos, então, trabalhar numericamente a fim de encontrar a configuração de parâmetros ótimos. As principais características destas distribuições são mostradas nas figuras 3.11 e 3.12.

Para as distribuições de circunferência e disco deslocadas observou-se que sempre quando $|Re[\beta]| = |Im[\beta]|$ os parâmetros ótimos são tais que $g_v = g_u$ e $\theta = \pi/4$, enquanto $g_v \neq g_u$ e $\theta \neq \pi/4$ quando $|Re[\beta]| \neq |Im[\beta]|$ (gráficos inferiores da figura 3.12(b)). Este resultado mostra que para a grande maioria das distribuições aqui investigadas a estratégia de otimização usando um único parâmetro não é suficiente para atingir a mais alta eficiência possível.

Observamos também que ao aumentarmos o parâmetro de compressão r e o raio R da distribuição nos aproximamos da fidelidade do PTVC original para distribuições centradas em qualquer β. No entanto, e realmente surpreendente, ao se deslocar a distribuição ao longo do eixo real (imaginário), a fidelidade média ótima tende a um limite assintótico consideravelmente melhor do que o previsto pelo PTVC original (gráficos a esquerda nas figuras 3.11(a) e 3.11(b)). E a medida que movemos o centro da distribuição para longe dos eixo real (imaginário), a fidelidade média ótima assintótica começa a se aproximar da fidelidade média dada pelo PTVC original. Para $\arg(\beta) = 30°$ a fidelidade média ótima assintótica é indistinguível da fidelidade média do PTVC original (gráficos à direita nas figuras 3.11(a) e 3.11(b)).

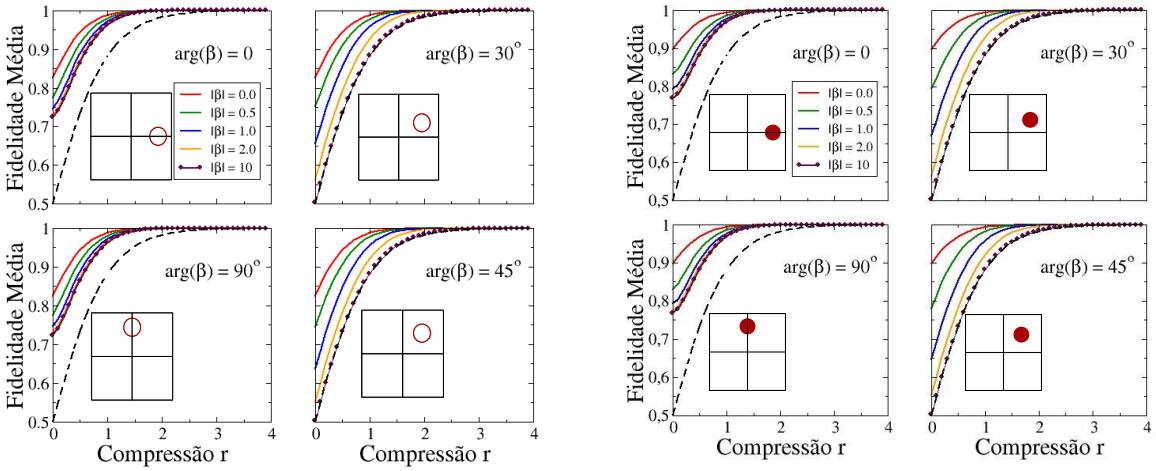


Figura 3.11: *(a) Os gráficos mostram a fidelidade média ótima como função do parâmetro de compressão r para várias distribuições circulares de raio $R = 0.5$ deslocadas por $\beta = |\beta|e^{\arg(\beta)}$. $|\beta|$ aumenta de cima para baixo (curvas solidas) e $\arg(\beta)$ é mostrado nos gráficos. A curva tracejada dá a fidelidade do PTVC original. Para um baixa compressão r, note que à medida que aumentamos $|\beta|$ para $\arg(\beta) = 0$ ou $\pi/2$ a fidelidade média ótima tende a valores muito superiores ao previsto pelo PTVC original. Esse fato interessante não acontece se o centro da distribuição se afasta dos eixos real e imaginário, onde as curvas da fidelidade do PTVC original e a fidelidade média ótima para $|\beta| = 10$ já não podem ser distinguidas. (b) A fidelidade média ótima como função da compressão r para várias distribuições em disco de raio $R = 0.5$ deslocadas em $\beta = |\beta|e^{\arg(\beta)}$. $|\beta|$ aumenta de cima para baixo (curvas sólidas) e $\arg(\beta)$ são ilustrados nos gráficos. A curva tracejada é a fidelidade média do PTVC original. As mesmas características destacadas na legenda da figura 3.11(a) são encontradas aqui.*

Estados em uma distribuição Gaussiana

Consideremos agora que o conjunto de estados de entrada com Alice é descrito por uma distribuição Gaussiana com variância $1/(2\lambda)$ e centrada em β,

$$P_G(\alpha) = (\lambda/\pi)\exp\left(-\lambda|\alpha-\beta|^2\right). \tag{3.29}$$

Quando $\beta = 0$ a distribuição está centrada no estado de vácuo e para $\beta \neq 0$ a distribuição estará centrada no estado coerente $|\beta\rangle$ (veja figura 3.14). Além disso, a medida que aumentamos λ (diminuindo a variância) a distribuição se aproxima de um único ponto, β, e quando $\lambda \to 0$ nós temos uma distribuição uniforme que cobre todo o plano complexo.

Inserindo a eq. (3.29) na eq. (2.38) podemos facilmente calcular a fidelidade média para um conjunto de estados coerentes de entrada distribuídos de acordo com uma distribuição Gaussiana centrada em β,

$$F_m^G = \frac{\lambda \exp\left[\frac{-\lambda f_1(\theta+\pi/2,g_u)Re[\beta]^2}{f_1(\theta+\pi/2,g_u)+\lambda f_2(\theta-\pi/2,g_u)}\right]}{\sqrt{f_1(\theta+\pi/2,g_u)+\lambda f_2(\theta-\pi/2,g_u)}} \frac{\exp\left[\frac{-\lambda f_1(\theta,g_v)Im[\beta]^2}{f_1(\theta,g_v)+\lambda f_2(\theta,g_v)}\right]}{\sqrt{f_1(\theta,g_v)+\lambda f_2(\theta,g_v)}}. \tag{3.30}$$

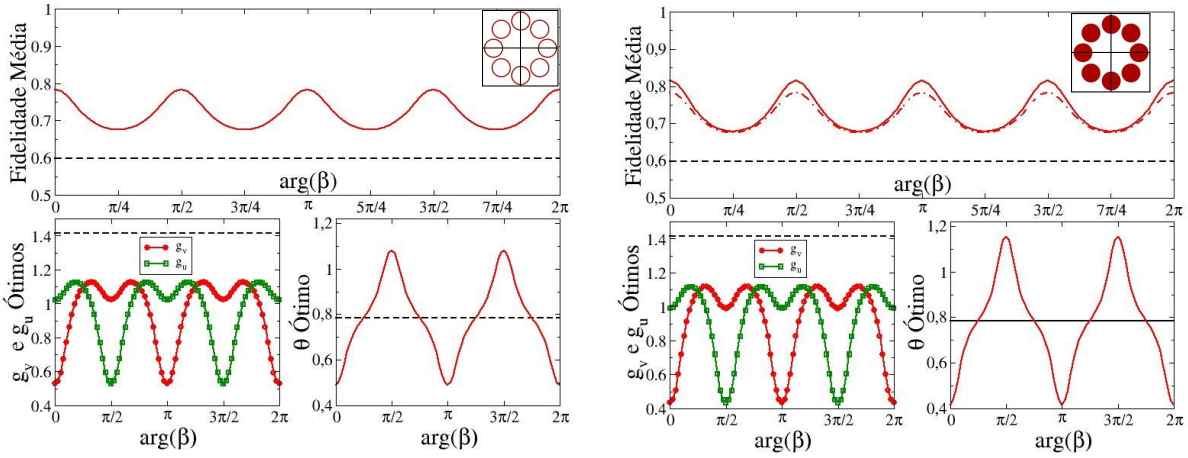


Figura 3.12: *(a) Aqui os estados de entrada são dados por uma distribuição uniforme em forma de circunferência com raio* $R = 0.5$, $|\beta| = 1.5$, *e parâmetro de compressão* $r = 0.2$. *Gráfico de cima: A fidelidade média ótima em função do* $\arg(\beta)$. *O gráfico intermo mostra as distribuições de maior (centradas nos eixos real e imaginário) e menor (*$\arg(\beta) = \pm 45^o$ *e* $\arg(\beta) = \pm 135^o$*) fidelidades média ótima. Gráfico inferior à esquerda:* g_v *e* g_u *ótimos, cujos valores estão em quadratura (com defasagem de* 90^o*). Note que eles só são iguais para* $\arg(\beta) = \pm 45^o$ *e* $\arg(\beta) = \pm 135^o$*, ou seja, quando* $|Re(\beta)| = |Im(\beta)|$. *Gráfico inferior direito:* θ *ótimo, que é igual* $\theta = 45^o$ *nos mesmos pontos onde* $g_v = g_u$. *Todas as curvas tracejadas correspondem ao resultado do PTVC original. (b) Distribuição de disco com raio* $R = 0.5$, *deslocada de* $|\beta| = 1.5$, *e compressão* $r = 0.2$. *Gráfico de cima: Fidelidade média ótima como função de* $\arg(\beta)$ *(curva vermelha sólida). Para comparação, mostramos a fidelidade média ótima para uma distribuição em circunferência com os mesmos parâmetros (curva ponto-tracejada vermelha). O gráfico interno acima mostra as distribuições de maior (centradas nos eixos real e imaginário) e de menor (*$\arg(\beta) = \pm 45^o$ *e* $\arg(\beta) = \pm 135^o$*) fidelidades média ótima. Gráfico inferior à esquerda:* g_v *e* g_u *ótimos, cujos valores estão em quadraturas (defasados em* 90^o*). Note que eles só são iguais para* $\arg(\beta) = \pm 45^o$ *e* $\arg(\beta) = \pm 135^o$*, ou seja, quando* $|Re(\beta)| = |Im(\beta)|$. *Gráfico inferior à direita:* θ *ótimo, que é igual* $\theta = 45^o$ *nos mesmos pontos onde* $g_v = g_u$. *Todas as curvas tracejadas correspondem aos valores dados pela fidelidade média do PTVC original.*

Para distribuições Gaussianas centradas no estado de vácuo ($\beta = 0$), a maximização da fidelidade média leva aos parâmetros ótimos $\theta^{ot} = \pi/4$ e $g_v^{ot} = g_v^{ot} = g$, onde g é (Braunstein et al., 2001)

$$g = \frac{2\sqrt{2} + \lambda\sqrt{2}\sinh(2r)}{2 + \lambda + \lambda\cosh(2r)}. \tag{3.31}$$

Na figura 3.13 mostramos como a fidelidade média ótima depende do emaranhamento do canal para várias distribuições Gaussianas diferentes centradas no estado de vácuo $\beta = 0$. Tal como esperado, a medida que diminuímos λ, cobrindo todo o plano complexo, recuperamos o resultado do PTVC original.

Ao trabalharmos com distribuições Gaussianas deslocadas por $\beta \neq 0$, não podemos obter uma solução analítica simples para o problema de otimização e teremos

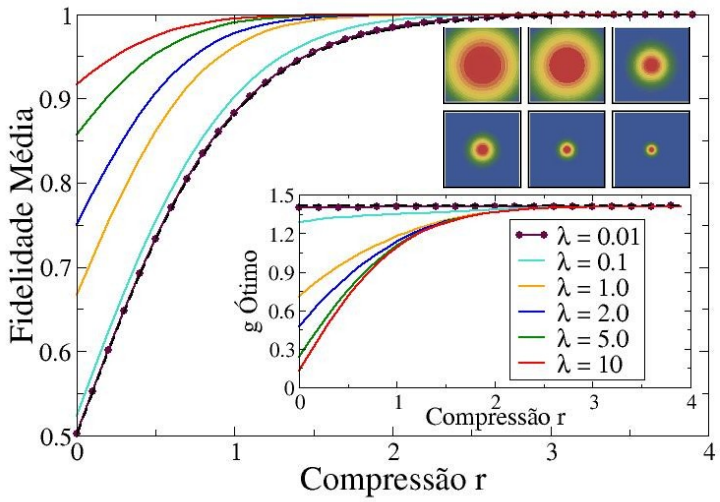


Figura 3.13: *As curvas solidas correspondem a fidelidade média ótima em função do emaranhamento do canal (compressão r) para um conjunto de estados de entrada dado por uma distribuição gaussiana centrada na origem com variância* $1/(2\lambda)$*, com* λ *aumentando de baixo para cima. Curvas tracejadas: fidelidade média dada pelo PTVC original, que é indistinguível da distribuição Gaussiana com* $\lambda = 0.01$*. Gráfico interno superior: Gráficos de densidade para várias distribuições Gaussianas, onde a variância diminui (*λ *aumenta) da esquerda para a direita. Gráfico interno inferior: O ganho ótimo* $g_v = g_u = g$ *resultando nas fidelidades ótimas mostradas no gráfico principal. Aqui,* λ *aumenta de cima para baixo e a curva tracejada é g de acordo com PTVC original, que é indistinguível para uma distribuição com* $\lambda = 0.01$*. O parâmetro* θ *ótimo é sempre* $\pi/4$*.*

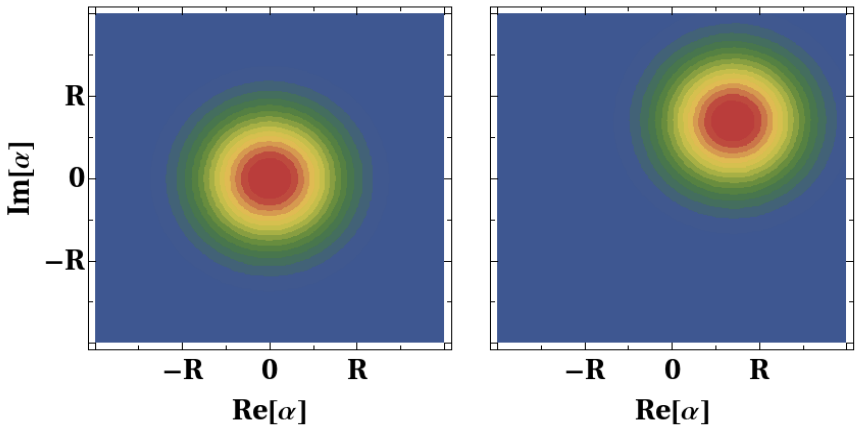
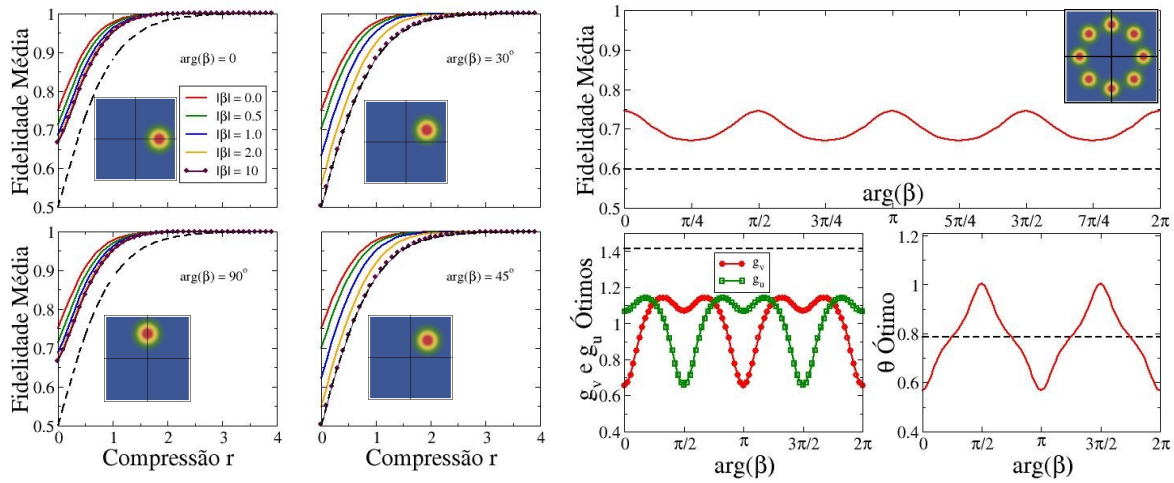


Figura 3.14: *Representação esquemática de possíveis distribuições Gaussianas* $P_G(\alpha)$ *para os estados de entrada disponíveis para Alice. Esquerda: Distribuição Gaussiana centrada no estado vácuo. Direita: Distribuição Gaussiana centrada no estado* $|\beta\rangle$*,* $\beta \neq 0$*.*

que utilizar métodos numéricos. Nas figuras 3.15(a) e 3.15(b) mostramos o resultado de diversos cálculos numéricos, que resultaram na fidelidade média ótima e nas configurações ótimas para distribuições Gaussianas deslocadas de várias maneiras diferentes a partir da origem do plano complexo. Os comportamentos qualitativos são muito semelhantes aos já discutidos para as distribuições de circunferência e disco. Uma análise mais detalhada

pode ser encontrada nas legendas das figuras 3.15(a) e 3.15(b).



(a) (b)

Figura 3.15: *(a) Fidelidade média ótima em função do parâmetro de compressão r para distribuições Gaussianas com variâncias* $1/(2\lambda)$*,* $\lambda = 2.0$*, e centradas em* $\beta = |\beta|e^{\arg(\beta)}$*.* $|\beta|$ *aumenta de cima para baixo (curva sólida) e* $\arg(\beta)$ *são mostrados nos gráficos internos. A curva tracejada é a fidelidade do PTVC original. Para um parâmetro de compressão pequeno, note que a medida que aumentamos* $|\beta|$ *para* $\arg(\beta) = 0$ *ou* $\pi/2$ *(gráficos à esquerda) a fidelidade média ótima tende a valores muito superiores ao previstos pelo PTVC original. Esse fato interessante não ocorre se o centro da distribuição se afasta do eixo real (imaginário) (gráficos à direita), onde as curvas da fidelidade média do PTVC original e* $|\beta| = 10$ *são indistinguíveis. (b) Distribuição Gaussiana com variância* $1/(2\lambda)$*,* $\lambda = 2.0$*, centrada em* $\beta = |\beta|e^{\arg(\beta)}$ *com* $|\beta| = 1.5$*. A compressão do canal é fixada em* $r = 0.2$*. Gráfico superior: Fidelidade média ótima como função do* $\arg(\beta)$ *(curvas sólidas). O gráfico interno mostra distribuições Gaussianas com maior (centradas nos eixos real e imaginário) e menor (*$\arg(\beta) = \pm 45^o$ *e* $\arg(\beta) = \pm 135^o$*) fidelidades média ótima. Gráfico inferior à esquerda:* g_v *e* g_u *ótimos, cujos valores estão em quadraturas (estão defasados em* 90^o*). Note que eles só são iguais para* $\arg(\beta) = \pm 45^o$ *e* $\arg(\beta) = \pm 135^o$*, ou seja, quando* $|Re(\beta)| = |Im(\beta)|$*. Gráfico inferior à direita:* θ *ótimo é* $\theta = 45^o$ *nos mesmos pontos onde* $g_v = g_u$*. Todas as curvas tracejadas correspondem aos valores do PTVC original.*

3.3 Discussão

Até aqui nesta Tese estudamos extensivamente modificações no PTVC original (Braunstein and Kimble, 1998), a fim de aumentar sua eficiência no teletransporte de estados coerentes levando em conta dois fatos inerentemente presentes em qualquer implementação real. O primeiro deles é o fato de que Alice e Bob sempre lidam com recursos de emaranhamento finito (estados comprimidos de dois modos) e o segundo está relacionado com o fato de que o conjunto de estados coerentes possíveis de Alice não cobrem todo o plano complexo.

Depois de estudar várias distribuições de probabilidades diferentes para o conjunto de estados de entrada com Alice, nós mostramos que ganhos consideráveis

de eficiência são obtidos para todas as distribuições se introduzirmos modificações na configuração inicial. A primeira delas foi a modificação da transmitância do divisor de feixes, a qual pode ser ajustada da forma que desejarmos. A outra modificação foi a possibilidade de escolher livremente os deslocamentos nas quadraturas, ou seja, na posição e momento, do estado de saída (teletransportado) de Bob. Ao permitir que essas três ações possam ser ajustadas de forma independente, nós fomos capazes de obter ganhos consideráveis em termos de eficiência quando comparado com o previsto pelo protocolo original.

Também comparamos estratégias de otimização de três parâmetros em relação a estratégia padrão de um parâmetro usada por Braunstein et al. (2001); Ide et al. (2002); van Loock and Braunstein (1999), onde o ganho na posição e no momento não são independentes. Para certos tipos de distribuição de estados de entrada de Alice, qual sejam, distribuições centradas no estado de vácuo e com simetria circular, demonstramos que a estratégia de otimização de três parâmetros se reduz à de um parâmetro. No entanto, quando a simetria circular é quebrada, a estratégia de três parâmetros é crucial para se obter um protocolo de teletransporte mais eficiente. Na verdade, mostramos que para distribuições onde há quebra da simetria circular, o caso de otimização de um parâmetro não dá um ganho significativo na eficiência se comparado com o PTVC original, enquanto nas mesmas condições a estratégia de três parâmetros dá ganhos consideráveis.

Além de importantes ganhos de eficiência com a estratégia de três parâmetros, também fomos capazes de identificar uma característica interessante para as distribuições com simetria circular deslocadas da origem centralizadas sobre os eixos real ou imaginário. Mostramos que essas distribuições atingem um maior ganho de eficiência quando comparadas a distribuições equivalentes centradas fora dos eixos real ou imaginário. Para distribuições com simetria circular centradas sobre os eixos real ou imaginário, nós mostramos que ao se aumentar a distância da distribuição de simetria circular em relação a origem (estado de vácuo), a fidelidade ótima tende para um valor limite que é maior do que a do protocolo original. Esse efeito é mais expressivo para os canais com baixo grau de emaranhamento e está ausente em distribuições centradas fora do eixo real e imaginário. Acreditamos que essas propriedades possam ser úteis na implementação de protocolos de distribuição de chaves quânticas em variáveis contínuas com base em estados coerentes (Elser et al., 2009; Grosshans and Grangier, 2002; Grosshans et al., 2003; Hirano et al., 2003; Jouguet et al., 2002; Ralph, 1999; Sych and Leuchs, 2010), onde ao invés de transmitir o estado coerente entre as partes envolvidas no esquema de distribuição de chaves, nós simplesmente o teletransportamos.

Além disso, em nossos cálculos supusemos um estado de vácuo comprimido de dois modos como nosso recurso de emaranhamento e um conjunto de estados dados por estados coerentes. Essas duas escolhas são ditadas pelo fato de serem os recurso mais utilizados em implementações reais de teletransporte em variáveis contínuas

(Braunstein and Kimble, 1998; Furusawa et al., 1998). Adicionalmente, o formalismo apresentado neste capítulo pode ser adaptado a qualquer estado de entrada e a todo tipo de canal quântico. Essas alterações são matematicamente implementadas simplesmente substituindo as funções de onda do estado de entrada e do canal na eq. (3.11) pelas funções de onda do novo estado de entrada e do novo canal.

Finalmente, gostaríamos de chamar a atenção para uma determinada extensão da pequisa apresentada aqui. Seria uma análise da estratégia de otimização de três parâmetros supondo que Alice e Bob compartilhem canais quânticos dados por estados mistos, ao invés de canais puros como fizemos aqui.

No próximo capítulo estenderemos o nosso estudo do PTVC. Adicionando um canal, estado comprimido de dois modos compartilhado entre Alice e Bob, paralelamente ao canal já existente no PTVC padrão. Esperando que dessa maneira haja um aumento significativo na eficiência do teletransporte em relação aos resultados encontrados neste capítulo.

Capítulo 4

Teletransporte com dois Canais

Dada a impossibilidade de se obter um canal maximamente emaranhado em variáveis contínuas, e por consequência a impossibilidade de se obter 100% de eficiência no PTVC para uma distribuição completamente desconhecida de estados com Alice, surge, então, uma extensão natural do estudo realizado no capítulo 3: a utilização de múltiplos canais parcialmente emaranhados para realizar o PTVC com uma maior eficiência.

Um exemplo bem sucedido da utilização de múltiplos canais em variáveis discretas é mostrado por Rigolin (2009), que faz uso de n canais parcialmente emaranhados, dispostos de forma sequencial, de modo que o estado teletransportado é o estado de entrada do teletransporte subsequente. Neste protocolo, a cada teletransporte o nível de emaranhamento do canal decai, resultando em alta eficiência e probabilidade de sucesso. O análogo desse protocolo para variáveis contínuas pode ser visto em Yonezawa et al. (2007). Yonezawa et al. (2007) mostra que independentemente do nível de emaranhamento dos canais subsequentes, a eficiência do protocolo a partir da segunda sequência de teletransporte cai próxima ao limite clássico. Isso mostra que a utilização de n canais em teletransportes sequenciais usando sistemas de variáveis contínuas é inviável para o aumento da eficiência.

Esses resultados põem em xeque o uso de múltiplos canais em sistemas de variáveis contínuas, pelo menos da forma como apresentada por Yonezawa et al. (2007). No entanto, uma mudança de paradigma introduzida por Andersen and Ralph (2013) mostrou o poder do uso de múltiplos canais no teletransporte de um estado descrito por variáveis contínuas. Os autores fazem uso do chamado sistema híbrido, teletransportando um estado coerente através de n canais emaranhados discretos (estados de Bell). Utilizando cerca de 50 canais discretos os autores conseguem obter uma eficiência de cerca de 99.2% no teletransporte do estado. Para realizar tal feito, os autores "dividem" o estado em n modos, com ajuda de divisores de feixe, combinando esses n modos com n canais discretos e teletransportando esses modos. Após o teletransporte dos modos, Bob recombina esses modos com ajuda de divisores de feixe (DF), medindo os $n-1$ estados na base do estado de vácuo, alcançando assim uma grande eficiência no teletransporte. A ideia por trás desse

protocolo é dividir a informação do estado coerente em n partes e transmitir cada uma dessas partes por um canal discreto. Bob, após a transmissão, faz as operações inversas implementadas por Alice a fim de obter toda a informação do estado outrora com ela.

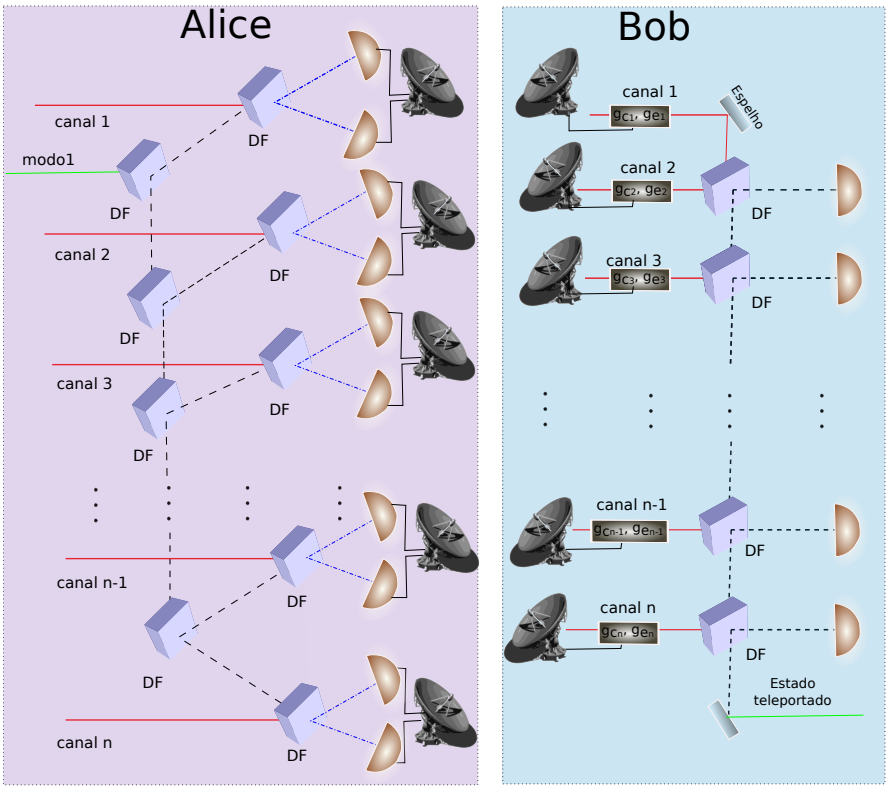


Figura 4.1: *Desenho esquemático dos possíveis arranjos de Alice para a combinação de canais. PTVC com canais paralelos (PTVCCP): Alice "divide" o estado a ser teletransportado em n partes (linha verde, modo 1) através de divisores de feixes (DF), combinando essas n partes com seus n modos emaranhados (linhas vermelhas). Após essa combinação Alice realiza as medidas em seus $2n$ modos, e informa a Bob os resultados destas medidas. Bob realiza os deslocamentos em seus canais, os quais dependem dos resultados das medidas de Alice, combinando-os dois a dois através de DF. Por fim, Bob mede seus $n-1$ modos restando, então, apenas o estado outrora pertencente a Alice.*

Com base no protocolo híbrido de Andersen and Ralph (2013), podemos criar um PTVC que utiliza n canais contínuos[1] parcialmente emaranhados para realizar o teletransporte ao invés de canais discretos. O design desse protocolo (veja figura 4.1) é inspirado no protocolo de Andersen and Ralph (2013). Ele consiste de $n-1$ DF usados por Alice de modo a "dividir" o estado a ser teletransportado em n modos, e combinando esses n modos com n modos dos canais através de n DF (cada canal é um estado comprimido de dois modos, um modo pertencendo a Bob e outro a Alice). Alice realiza a medida nos seus $2n$ modos e envia o resultado dessas medidas a Bob. Ao receber o resultado dessas medidas, Bob realiza operações em seus modos e em seguida combina os canais dois a dois através de um DF medindo uma saída e combinando a outra com um outro canal

[1]Por canais contínuos, queremos dizer estados emaranhados que são descritos por variáveis contínuas.

através de um outro DF. Ele repete esse procedimento n vezes (uma vez para cada modo), realizando medidas em $n-1$ modos, restando então apenas o estado teletransportado.

Como podemos ver na figura 4.1, esse protocolo trabalha com n canais em paralelo. Desse modo, a partir daqui, iremos nos referir a ele como protocolo de teletransporte em variáveis contínuas com canais em paralelo ou PTVCCP. Assim como no protocolo híbrido, desejamos dividir a informação do estado e transmiti-la pelos n canais com uma eficiência maior do que a conseguida por Yonezawa et al. (2007). Desse modo, nesse capítulo iremos proceder com uma análise semelhante à realizada no capítulo anterior. Na seção 4.1, estudamos o PTVCCP qualitativamente e quantitativamente e mostramos seu melhor desempenho frente ao protocolo sequencial apresentado por Yonezawa et al. (2007). Investigamos, também, várias distribuições de probabilidade associadas ao estado de entrada de Alice, comparando esses resultados com os obtidos no capítulo anterior.

4.1 PTVC com canais em paralelo

Nessa seção descrevemos nosso PTVCCP primeiramente através de uma análise qualitativa, definindo os parâmetros a serem utilizados no protocolo. Assim como já fizemos, deixamos livres os parâmetros de interação (DF e deslocamentos), de modo a estudar o efeito de alterações nesses parâmetros no protocolo. Em seguida, partiremos para a análise quantitativa do PTVCCP. Com isso obtemos na representação de Schrödinger o estado final de Bob após o teletransporte e a eficiência do protocolo, quantificada através da fidelidade e maximizada em termos dos parâmetros de interação. O PTVCCP foi concebido para n canais (ver figura 4.1). No entanto, a adição de cada novo canal aumenta a complexidade do cálculo de maneira expressiva. Portanto, nessa Tese, iremos nos ater ao estudo de dois canais paralelos.

4.1.1 Análise Qualitativa

Nesse protocolo temos dois estados comprimidos de dois modos com compressões r_1 e r_2, que são compartilhados entre Alice e Bob. Os modos 3 e 4 são entregues a Alice enquanto os modos 5 e 6 a Bob (veja figura 4.2). Alice, ao receber o estado a ser teletransportado (representado pelo modo 1), combina-o com o modo 2 (estado de vácuo) através de um divisor de feixes (DF(θ)). Isso equivale a "dividir" o feixe em dois, e é representado pela interação do estado a ser teletransportado com o estado de vácuo. Dando prosseguimento ao protocolo, Alice combina o modo 3 com o modo a e o modo 4 com o modo b através de divisores de feixes (DF(η) e DF(γ), respectivamente). Em seguida Alice mede as posições (quadraturas do campo eletromagnético) dos modos e e f e os momentos (quadraturas do campo eletromagnético) dos modos c e d. Os resultados dessas medidas são representados por $\tilde{x}_e$, $\tilde{x}_f$, $\tilde{p}_c$ e $\tilde{p}_d$, sendo então comunicados a Bob de

maneira clássica.

Com a informação das medidas realizadas por Alice, Bob realiza deslocamentos nas posições ($x_5 \to x_5 + g_e\tilde{x}_e$ e $x_6 \to x_6 + g_f\tilde{x}_f$) e nos momentos ($p_5 \to p_5 + g_c\tilde{p}_c$ e $p_6 \to p_6 + g_d\tilde{p}_d$) dos modos 5 e 6. Após realizar os deslocamentos dos modos, Bob interage seus estados através de DF(ξ) e, após essa interação, ele realiza a medida do modo j encerando assim o protocolo. Se supormos que todos os parâmetros do PTVCCP sejam iguais ao do protocolo original (Braunstein and Kimble, 1998), ou seja, $g_i = \sqrt{2}$ onde $i = \{c, d, e, f\}$ e $\zeta = \pi/4$ onde $\zeta = \{\theta, \eta, \gamma, \xi\}$, para canais maximamente emaranhados ($r_1 \to \infty$ e $r_2 \to \infty$) o estado de Alice será perfeitamente teletransportado. Ou seja, toda informação outrora contida no estado de Alice (modo 1) estará agora no estado de Bob (modo k).

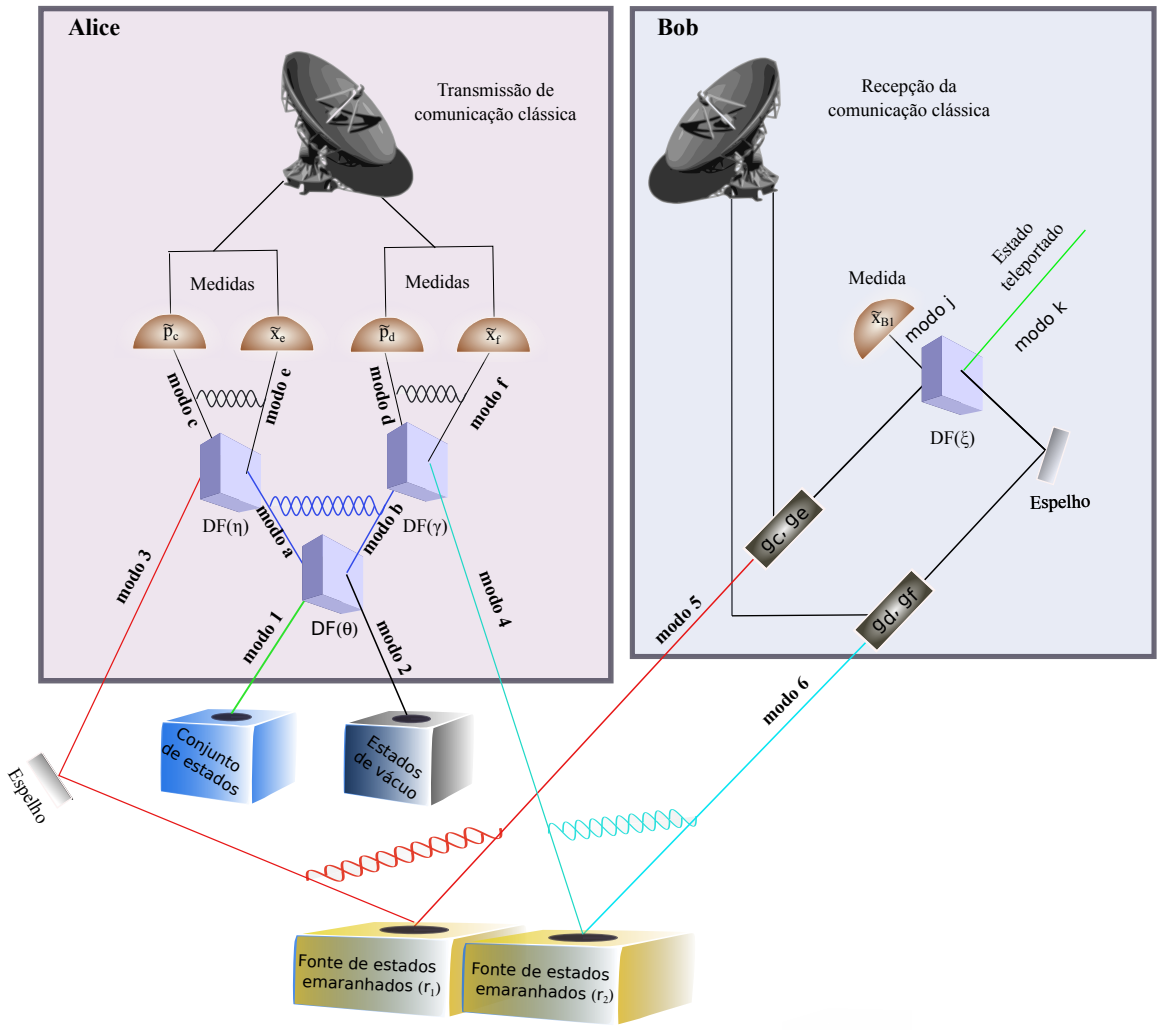


Figura 4.2: *Desenho esquemático do procedimento do PTVCCP para dois canais. Aqui, fixaremos λ e a compressão r, e a otimização da fidelidade média F_m será implementada através dos três parâmetros livres, θ, g_v, e g_u, resultando em uma F_m que depende de r e λ. Veja o texto para maiores detalhes.*

Realisticamente não há como termos compressão infinita. E como no caso do

teletransporte padrão (capítulo 3), não há garantia de que as escolhas das transmitâncias dos divisores de feixes ($\cos^2(\zeta) = 1/2$), dos deslocamentos e do ganho sejam os mesmos para todas as combinações de compressões finitas (r_1 e r_2) e distribuições de probabilidade do conjunto de estados disponíveis a Alice. Portanto, como no capítulo 3, a fim de procurar um protocolo ideal para parâmetros de compressão r_1 e r_2 finitos, nós deixamos os divisores de feixes com transmitância arbitrária (DF(ζ)), onde $0 < \zeta < \pi/2$ (veja figura 4.2). Além disso, os deslocamentos das quadraturas e os ganhos implementados por Bob, após ser informado dos resultados das medidas de Alice, também serão escolhidos de forma independente a fim de otimizar o protocolo.

4.1.2 Análise Quantitativa

Apresentamos agora os pormenores da análise matemática de nosso protocolo, no qual os parâmetros θ, η, γ, ξ, g_c, g_d, g_e e g_f são deixados livres (veja figura 4.2). Assim como no capítulo 3, usamos indistintamente as palavras kets, estados e modos para nos referir ao mesmo objeto, os modos do campo eletromagnético quantizado.

De acordo com o quarto postulado da mecânica quântica exposto no capítulo 2, podemos escrever o estado do sistema antes do início do teletransporte da seguinte forma

$$|\Lambda\rangle = |\varphi\rangle \otimes |0\rangle \otimes |\Phi_1\rangle \otimes |\Phi_2\rangle. \tag{4.1}$$

Aqui $|\varphi\rangle$ é o estado que Alice deseja teletransportar (modo 1, veja figura 4.2), o estado $|0\rangle$ é o estado de vácuo e os estados $|\Phi_1\rangle$ e $|\Phi_2\rangle$ são os canais cujos modos 3 e 4 pertencem a Alice e os modos 5 e 6 a Bob. Podemos reescrever o estado inicial na base da posição usando a equação (2.3):

$$|\Lambda\rangle = \left(\frac{2}{\pi}\right)^{\frac{1}{4}} \int dx_1 dx_2 dx_3 dx_4 dx_5 dx_6 e^{x_2^2} \varphi(x_1)\Phi_1(x_3, x_4)\Phi_2(x_5, x_6)|x_1, x_2, x_3, x_4, x_5, x_6\rangle \tag{4.2}$$

onde $\varphi(x_1) = \langle x|\varphi\rangle$, $\langle x_2|0\rangle = (2/\pi)^{1/4}\mathrm{H}_0(\sqrt{2}x_2)e^{-x_2^2}$, $\Phi_1(x_3, x_4) = \langle x_3, x_4|\Phi_1\rangle$ e $\Phi_2(x_5, x_6) = \langle x_5, x_6|\Phi_2\rangle$, com $\mathrm{H}_0(\sqrt{2}x_2) = 1$ sendo o primeiro polinômio de Hermite. Salvo dito de outra forma, a ordenação dos estados será mantida da seguinte forma: |modo 1, modo 2, modo 3, modo 4, modo 5, modo 6$\rangle$. O primeiro passo do protocolo consiste em "dividir" o estado a ser teletransportado em duas partes. Isso é "feito" combinando o modo 1 com o modo 2 através de um divisor de feixes (DF) com transmitância $\cos^2(\theta)$. A operação realizada pelo divisor de feixes é representada pela aplicação do operador (2.82). Após a

aplicação do operador o estado (4.2) pode ser escrito como

$$|\Lambda'\rangle = \left(\frac{2}{\pi}\right)^{\frac{1}{4}} \int dx_a dx_b dx_3 dx_4 dx_5 dx_6 e^{-(x_a\cos(\theta)-x_b\sin(\theta))^2} \varphi(x_a\sin(\theta)+x_b\cos(\theta)) \times \Phi_1(x_3,x_4)\Phi_2(x_5,x_6)|x_a,x_b,x_3,x_4,x_5,x_6\rangle, \quad (4.3)$$

onde $x_a = x_1\sin(\theta) + x_2\cos(\theta)$ e $x_b = x_1\cos(\theta) - x_2\sin(\theta)$.

O segundo passo do protocolo consiste nas interações com os canais. Para tanto, Alice envia o modo a e o modo 3 (modo do canal pertencente a ela) a um divisor de feixes (DF) com transmitância $\cos^2(\eta)$ no mesmo instante em que envia o modo b e o modo 4 (outro modo do canal também pertencente a ela) a outro divisor de feixes (DF) com transmitância $\cos^2(\gamma)$. Logo após as aplicações do operador que representa o divisor de feixes (2.82), o estado (4.3) pode ser escrito como

$$\begin{aligned}|\Lambda''\rangle = & \left(\frac{2}{\pi}\right)^{\frac{1}{4}} \int dx_c dx_d dx_e dx_f dx_5 dx_6 \exp\{-(x_c\sin(\eta)\cos(\theta) + x_e\cos(\eta)\cos(\theta) \\ & -x_d\sin(\gamma)\sin(\theta) - x_f\cos(\gamma)\sin(\theta))^2\}\varphi\left(x_c\sin(\eta)\sin(\theta) + x_e\cos(\eta)\sin(\theta)\right. \\ & \left.+x_d\sin(\gamma)\cos(\theta) + x_f\cos(\gamma)\cos(\theta)\right)\Phi_1\left(x_c\cos(\eta) - x_e\sin(\eta), x_5\right) \\ & \times\Phi_2\left(x_d\cos(\gamma) - x_f\sin(\gamma), x_6\right)|x_c,x_d,x_e,x_f,x_5,x_6\rangle, \end{aligned} \quad (4.4)$$

onde $x_c = x_a\sin(\eta) + x_3\cos(\eta)$, $x_d = x_b\sin(\gamma) + x_4\cos(\gamma)$, $x_e = x_a\cos(\eta) - x_3\sin(\eta)$ e $x_f = x_b\cos(\gamma) - x_4\sin(\gamma)$.

O próximo passo do protocolo consiste em medir as posições dos modos e e f e os momentos dos modos c e d. A medida das quadraturas do campo é feita por detecção homódina, a mesma realizada no capítulo anterior, de modo que as fotocorrentes atribuem números reais para as quadraturas $\tilde{p}_c$, $\tilde{x}_e$, $\tilde{p}_d$ e $\tilde{x}_f$. Para medir os momentos, Alice deve projetar os modos c e d na base dos momentos, sendo então conveniente reescrever estes modos da equação (4.4) na base dos momentos. Para mudarmos a base faremos uso da relação (2.49). Assim, a eq. (4.4) pode ser escrita como

$$\begin{aligned}|\Lambda''\rangle = & \left(\frac{2}{\pi}\right)^{\frac{1}{4}} \frac{1}{\pi} \int dx_c dx_d dx_e dx_f dx_5 dx_6 dp_c dp_d \exp\{-[(x_c\sin(\eta) + x_e\cos(\eta))\cos(\theta) \\ & -(x_d\sin(\gamma) + x_f\cos(\gamma))\sin(\theta)]^2\}\varphi\left((x_c\sin(\eta) + x_e\cos(\eta))\sin(\theta) + (x_d\sin(\gamma)\right. \\ & \left.+x_f\cos(\gamma))\cos(\theta)\right)\Phi_1\left(x_c\cos(\eta) - x_e\sin(\eta), x_5\right)\Phi_2\left(x_d\cos(\gamma) - x_f\sin(\gamma), x_6\right) \\ & \times e^{-2ix_cp_c}e^{-2ix_dp_d}|p_c,p_d,x_e,x_f,x_5,x_6\rangle. \end{aligned} \quad (4.5)$$

O estado total após o fim da medida é

$$|\Lambda_1\rangle = \frac{\hat{P}_{\tilde{p}_c,\tilde{p}_d,\tilde{x}_e,\tilde{x}_f}|\Lambda''\rangle}{\sqrt{\mathbb{P}(\tilde{p}_c,\tilde{p}_d,\tilde{x}_e,\tilde{x}_f)}}, \quad (4.6)$$

onde $\hat{P}_{\tilde{p}_c,\tilde{p}_d,\tilde{x}_e,\tilde{x}_f} = |\tilde{p}_c,\tilde{p}_d,\tilde{x}_e,\tilde{x}_f\rangle\langle\tilde{p}_c,\tilde{p}_d,\tilde{x}_e,\tilde{x}_f| \otimes \mathbb{1}_5 \otimes \mathbb{1}_6$ é o projetor que descreve as medidas, com $\mathbb{1}_5$ e $\mathbb{1}_6$ sendo os operadores identidade atuando sobre os modos 5 e 6, respectivamente, e $\mathbb{P}(\tilde{p}_c,\tilde{p}_d,\tilde{x}_e,\tilde{x}_f) = tr(|\Lambda''\rangle\langle\Lambda''|\hat{P}_{\tilde{p}_c,\tilde{p}_d,\tilde{x}_e,\tilde{x}_f})$ é a probabilidade obter os momentos $\tilde{p}_c$ e $\tilde{p}_d$ e as posições $\tilde{x}_e$ e $\tilde{x}_f$. Logo, o estado total após a medida é

$$|\Lambda_1\rangle = |\tilde{p}_c,\tilde{p}_d,\tilde{x}_e,\tilde{x}_f\rangle \otimes |\Xi'\rangle, \tag{4.7}$$

com o estado de Bob sendo dado por

$$\begin{aligned}|\Xi'\rangle \;=\; & \left(\frac{2}{\pi}\right)^{\frac{1}{4}} \frac{1}{\pi\sqrt{\mathbb{P}(\tilde{p}_c,\tilde{p}_d,\tilde{x}_e,\tilde{x}_f)}} \int dx_c dx_d dx_5 dx_6 \exp\{-\left[(x_c\sin(\eta)+\tilde{x}_e\cos(\eta))\cos(\theta)\right. \\ & \left.-(x_d\sin(\gamma)+\tilde{x}_f\cos(\gamma))\sin(\theta)\right]^2\}\varphi\left((x_c\sin(\eta)+\tilde{x}_e\cos(\eta))\sin(\theta)+(x_d\sin(\gamma)\right. \\ & \left.+\tilde{x}_f\cos(\gamma))\cos(\theta)\right)\Phi_1\left(x_c\cos(\eta)-\tilde{x}_e\sin(\eta),x_5\right)\Phi_2\left(x_d\cos(\gamma)-\tilde{x}_f\sin(\gamma),x_6\right) \\ & \times e^{-2ix_c\tilde{p}_c}e^{-2ix_d\tilde{p}_d}|x_5,x_6\rangle. \end{aligned} \tag{4.8}$$

Aqui

$$\mathbb{P}(\tilde{p}_c,\tilde{p}_d,\tilde{x}_e,\tilde{x}_f) = \int dx_5 dx_6 |\Lambda''(\tilde{p}_c,\tilde{p}_d,\tilde{x}_e,\tilde{x}_f,x_5,x_6)|^2 \tag{4.9}$$

e

$$\begin{aligned}&\Lambda''(\tilde{p}_c,\tilde{p}_d,\tilde{x}_e,\tilde{x}_f,x_5,x_6) = \langle\tilde{p}_c,\tilde{p}_d,\tilde{x}_e,\tilde{x}_f,x_5,x_6|\Lambda''\rangle = \left(\frac{2}{\pi}\right)^{\frac{1}{4}}\frac{1}{\pi}\int dx_c dx_d \\ &\times\exp\{-\left[(x_c\sin(\eta)+\tilde{x}_e\cos(\eta))\cos(\theta)-(x_d\sin(\gamma)+\tilde{x}_f\cos(\gamma))\sin(\theta)\right]^2\} \\ &\times\varphi\left((x_c\sin(\eta)+\tilde{x}_e\cos(\eta))\sin(\theta)+(x_d\sin(\gamma)+\tilde{x}_f\cos(\gamma))\cos(\theta)\right) \\ &\times\Phi_1\left(x_c\cos(\eta)-\tilde{x}_e\sin(\eta),x_5\right)\Phi_2\left(x_d\cos(\gamma)-\tilde{x}_f\sin(\gamma),x_6\right)e^{-2ix_c\tilde{p}_c-2ix_d\tilde{p}_d}. \end{aligned} \tag{4.10}$$

Essas últimas equações foram obtidas a partir da equação (4.7) utilizando as relações (2.47).

O quarto passo do protocolo consiste em Alice enviar a Bob por um canal clássico os resultados de suas medidas. Com essa informação Bob está apto a implementar o quinto passo do protocolo, o deslocamento das quadraturas dos modos 5 e 6 seguindo as regras, $x_5 \to x_5 + g_e\tilde{x}_e$, $p_5 \to p_5 + g_c\tilde{p}_c$, $x_6 \to x_6 + g_f\tilde{x}_f$ e $p_6 \to p_6 + g_d\tilde{p}_d$. Essa operação é realizada pelo operador deslocamento $\hat{D}(\alpha)$, onde para o modo 5 temos $\alpha = g_e\tilde{x}_e + ig_c\tilde{p}_c$ e para o modo 6 temos $\alpha = g_f\tilde{x}_f + ig_d\tilde{p}_d$. Assim, a aplicação desse operador resulta em

$$\begin{aligned}\hat{D}_5(g_e\tilde{x}_e+ig_c\tilde{p}_c)\hat{D}_6(g_f\tilde{x}_f+ig_d\tilde{p}_d)|x_5,x_6\rangle \;=\; & e^{ig_eg_c\tilde{x}_e\tilde{p}_c+ig_fg_d\tilde{x}_f\tilde{p}_d}e^{2ig_c\tilde{p}_cx_5}e^{2ig_d\tilde{p}_dx_6} \\ & \times|x_5+g_e\tilde{x}_e,x_6+g_f\tilde{x}_f\rangle. \end{aligned} \tag{4.11}$$

Realizando as mudanças de variável $x_5 \to x_5 - g_e\tilde{x}_e$ e $x_6 \to x_6 - g_f\tilde{x}_f$, o estado de Bob,

$|\Xi\rangle = \hat{D}_5(g_e\tilde{x}_e + ig_c\tilde{p}_c)\hat{D}_6(g_f\tilde{x}_f + ig_d\tilde{p}_d)|\Xi'\rangle$, pode ser escrito como

$$\begin{aligned}|\Xi\rangle &= \left(\frac{2}{\pi}\right)^{\frac{1}{4}} \frac{e^{-ig_eg_c\tilde{x}_e\tilde{p}_c - ig_fg_d\tilde{x}_f\tilde{p}_d}}{\pi\sqrt{\mathbb{P}(\tilde{p}_c,\tilde{p}_d,\tilde{x}_e,\tilde{x}_f)}} \int dx_c dx_d dx_5 dx_6 \exp\{-\left[(x_c\sin(\eta)+\tilde{x}_e\cos(\eta))\cos(\theta)\right.\\ &\left.-(x_d\sin(\gamma)+\tilde{x}_f\cos(\gamma))\sin(\theta)\right]^2\}\varphi\left((x_c\sin(\eta)+\tilde{x}_e\cos(\eta))\sin(\theta)+(x_d\sin(\gamma)\right.\\ &\left.+\tilde{x}_f\cos(\gamma))\cos(\theta)\right)\Phi_1\left(x_c\cos(\eta)-\tilde{x}_e\sin(\eta), x_5-g_e\tilde{x}_e\right)\Phi_2\left(x_d\cos(\gamma)-\tilde{x}_f\sin(\gamma), x_6\right.\\ &\left.-g_f\tilde{x}_f\right)e^{-2i(x_c-g_cx_5)\tilde{p}_c}e^{-2i(x_d-g_dx_6)\tilde{p}_d}|x_5,x_6\rangle. \qquad (4.12)\end{aligned}$$

Após realizar os deslocamentos, Bob dá início ao sexto passo do protocolo, interagindo seus dois modos através de um divisor de feixes (DF) de transmitância $\cos^2(\xi)$. Após esta operação podemos reescrever o estado de Bob como

$$\begin{aligned}|\Xi_1\rangle &= \left(\frac{2}{\pi}\right)^{\frac{1}{4}} \frac{e^{-ig_eg_c\tilde{x}_e\tilde{p}_c - ig_fg_d\tilde{x}_f\tilde{p}_d}}{\pi\sqrt{\mathbb{P}(\tilde{p}_c,\tilde{p}_d,\tilde{x}_e,\tilde{x}_f)}} \int dx_c dx_d dx_B dx_{B_1} \exp\{-\left[(x_c\sin(\eta)+\tilde{x}_e\cos(\eta))\cos(\theta)\right.\\ &\left.-(x_d\sin(\gamma)+\tilde{x}_f\cos(\gamma))\sin(\theta)\right]^2\}\varphi\left((x_c\sin(\eta)+\tilde{x}_e\cos(\eta))\sin(\theta)+(x_d\sin(\gamma)\right.\\ &\left.+\tilde{x}_f\cos(\gamma))\cos(\theta)\right)\Phi_1\left(x_c\cos(\eta)-\tilde{x}_e\sin(\eta), x_B\sin(\xi)+x_{B_1}\cos(\xi)-g_e\tilde{x}_e\right)\\ &\times\Phi_2\left(x_d\cos(\gamma)-\tilde{x}_f\sin(\gamma), x_B\cos(\xi)-x_{B_1}\sin(\xi)-g_f\tilde{x}_f\right)\\ &\times e^{-2i(x_c-g_c(x_B\sin(\xi)+x_{B_1}\cos(\xi)))\tilde{p}_c}e^{-2i(x_d-g_d(x_B\cos(\xi)-x_{B_1}\sin(\xi)))\tilde{p}_d}|x_B,x_{B_1}\rangle, \qquad (4.13)\end{aligned}$$

onde $x_5 = x_B\sin(\xi) + x_{B_1}\cos(\xi)$ e $x_6 = x_B\cos(\xi) - x_{B_1}\sin(\xi)$.

Bob então executa o sétimo e último passo do protocolo, realizando uma medida na posição do modo 6. Supondo que o resultado da medida seja $\tilde{x}_{B_1}$, o estado de Bob após o fim da medida é

$$|\Xi_2\rangle = \frac{\hat{P}_{\tilde{x}_{B_1}}|\Xi_1\rangle}{\sqrt{\mathbb{P}(\tilde{x}_{B_1})}}, \qquad (4.14)$$

onde $\hat{P}_{\tilde{x}_{B_1}} = \mathbb{1}_5 \otimes |\tilde{x}_{B_1}\rangle\langle\tilde{x}_{B_1}|$ é o projetor que descreve a medida, $\mathbb{1}_5$ o operador identidade atuando sobre o modo 5 e $\mathbb{P}(\tilde{x}_{B_1}) = tr(|\Xi_1\rangle\langle\Xi_1|\hat{P}_{\tilde{x}_{B_1}})$ a probabilidade de medida da posição $\tilde{x}_{B_1}$. Portanto, o estado após a medida é

$$|\Xi_2\rangle = |\Omega\rangle \otimes |\tilde{x}_{B_1}\rangle, \qquad (4.15)$$

de modo que ao final do protocolo o estado teletransportado em posse de Bob é

$$
\begin{aligned}
|\Omega\rangle \;=\; & \left(\frac{2}{\pi}\right)^{\frac{1}{4}} \frac{e^{-ig_e g_c \tilde{x}_e \tilde{p}_c - ig_f g_d \tilde{x}_f \tilde{p}_d}}{\pi\sqrt{\mathbb{P}(\tilde{p}_c,\tilde{p}_d,\tilde{x}_e,\tilde{x}_f)\mathbb{P}(\tilde{x}_{B_1})}} \int dx_c dx_d dx_B \exp\{-\left[(x_c\sin(\eta)+\tilde{x}_e\cos(\eta))\cos(\theta)\right. \\
& \left.-(x_d\sin(\gamma)+\tilde{x}_f\cos(\gamma))\sin(\theta)\right]^2\}\varphi\left((x_c\sin(\eta)+\tilde{x}_e\cos(\eta))\sin(\theta)+(x_d\sin(\gamma)\right. \\
& \left.+\tilde{x}_f\cos(\gamma))\cos(\theta)\right)\Phi_1\left(x_c\cos(\eta)-\tilde{x}_e\sin(\eta), x_B\sin(\xi)+\tilde{x}_{B_1}\cos(\xi)-g_e\tilde{x}_e\right) \\
& \times\Phi_2\left(x_d\cos(\gamma)-\tilde{x}_f\sin(\gamma), x_B\cos(\xi)-\tilde{x}_{B_1}\sin(\xi)-g_f\tilde{x}_f\right) \\
& \times e^{-2i(x_c-g_c(x_B\sin(\xi)+\tilde{x}_{B_1}\cos(\xi)))\tilde{p}_c} e^{-2i(x_d-g_d(x_B\cos(\xi)-\tilde{x}_{B_1}\sin(\xi)))\tilde{p}_d}|x_B\rangle, \qquad (4.16)
\end{aligned}
$$

com

$$
\mathbb{P}(\tilde{x}_{B_1}) = \int dx_B |\Xi_1(x_B,\tilde{x}_{B_1})|^2 \qquad (4.17)
$$

e

$$
\begin{aligned}
\Xi_1(x_B,\tilde{x}_{B_1}) \quad & = \langle x_B,\tilde{x}_{B_1}|\Xi_1\rangle = \left(\frac{2}{\pi}\right)^{\frac{1}{4}} \frac{e^{-ig_e g_c \tilde{x}_e \tilde{p}_c - ig_f g_d \tilde{x}_f \tilde{p}_d}}{\pi\sqrt{\mathbb{P}(\tilde{p}_c,\tilde{p}_d,\tilde{x}_e,\tilde{x}_f)}} \int dx_c dx_d \exp\{ \\
& -\left[(x_c\sin(\eta)+\tilde{x}_e\cos(\eta))\cos(\theta)-(x_d\sin(\gamma)+\tilde{x}_f\cos(\gamma))\sin(\theta)\right]^2\} \\
& \times\varphi\left((x_c\sin(\eta)+\tilde{x}_e\cos(\eta))\sin(\theta)+(x_d\sin(\gamma)+\tilde{x}_f\cos(\gamma))\cos(\theta)\right) \\
& \times\Phi_1\left(x_c\cos(\eta)-\tilde{x}_e\sin(\eta), x_B\sin(\xi)+\tilde{x}_{B_1}\cos(\xi)-g_e\tilde{x}_e\right) \\
& \times\Phi_2\left(x_d\cos(\gamma)-\tilde{x}_f\sin(\gamma), x_B\cos(\xi)-\tilde{x}_{B_1}\sin(\xi)-g_f\tilde{x}_f\right) \\
& \times e^{-2i(x_c-g_c(x_B\sin(\xi)+\tilde{x}_{B_1}\cos(\xi)))\tilde{p}_c} e^{-2i(x_d-g_d(x_B\cos(\xi)-\tilde{x}_{B_1}\sin(\xi)))\tilde{p}_d}. \qquad (4.18)
\end{aligned}
$$

Podemos reescrever o estado final de Bob, eq.(4.16), como

$$
\begin{aligned}
|\Omega\rangle \;=\; & \int dx_B \left(\left(\frac{2}{\pi}\right)^{\frac{1}{4}} \frac{e^{-ig_e g_c \tilde{x}_e \tilde{p}_c - ig_f g_d \tilde{x}_f \tilde{p}_d}}{\pi\sqrt{\mathbb{P}(\tilde{p}_c,\tilde{p}_d,\tilde{x}_e,\tilde{x}_f)\mathbb{P}(\tilde{x}_{B_1})}} \right. \\
& \times \int dx_c dx_d \exp\{-\left[(x_c\sin(\eta)+\tilde{x}_e\cos(\eta))\cos(\theta)\right. \\
& \left.-(x_d\sin(\gamma)+\tilde{x}_f\cos(\gamma))\sin(\theta)\right]^2\}\varphi\left((x_c\sin(\eta)+\tilde{x}_e\cos(\eta))\sin(\theta)+(x_d\sin(\gamma)\right. \\
& \left.+\tilde{x}_f\cos(\gamma))\cos(\theta)\right)\Phi_1\left(x_c\cos(\eta)-\tilde{x}_e\sin(\eta), x_B\sin(\xi)+\tilde{x}_{B_1}\cos(\xi)-g_e\tilde{x}_e\right) \\
& \times\Phi_2\left(x_d\cos(\gamma)-\tilde{x}_f\sin(\gamma), x_B\cos(\xi)-\tilde{x}_{B_1}\sin(\xi)-g_f\tilde{x}_f\right) \\
& \left. \times e^{-2i(x_c-g_c(x_B\sin(\xi)+\tilde{x}_{B_1}\cos(\xi)))\tilde{p}_c} e^{-2i(x_d-g_d(x_B\cos(\xi)-\tilde{x}_{B_1}\sin(\xi)))\tilde{p}_d} \right)|x_B\rangle \\
= \; & \int dx_B \chi(x_B)|x_B\rangle. \qquad (4.19)
\end{aligned}
$$

Note que assim com no capítulo anterior o estado final de Bob possui uma fase global $e^{-ig_e g_c \tilde{x}_e \tilde{p}_c - ig_f g_d \tilde{x}_f \tilde{p}_d}$ irrelevante. O estado final de Bob, eq.(4.19), juntamente com as equações (4.17) e (4.18) são gerais. Elas nos permitem obter o estado teletransportado

com Bob para qualquer estado de entrada e para quaisquer canais compartilhados entre Alice e Bob.

4.1.3 Resultados

Ao término do protocolo devemos checar o quão próximo o estado de Bob se encontra do estado de entrada. Como feito no capítulo anterior, faremos uso da fidelidade, eq. (2.37), para checar a eficiência do protocolo. Lembramos que o objetivo principal desse capítulo é obter um PTVC com múltiplos canais que supere os protocolos de múltiplos canais existentes (Yonezawa et al., 2007), utilizando os mesmos recursos ou menos.

Análise da Fidelidade

Para realizar a análise da eficiência do protocolo, restringimos o estado de entrada para um estado coerente (eq. (2.65)) e os canais como sendo estados de vácuo comprimido de dois modos (eq. (2.28)). Com estas escolhas podemos escrever a fidelidade, eq.(2.37), como

$$F\left(\alpha,\hat{\rho}_{out}\right)=\frac{8\exp\left[-\left(\frac{f_3(g_c,g_d,\eta,\gamma)}{f_4(g_c,g_d,\eta,\gamma)}Im^2\left[\alpha\right]+\frac{f_3\left(g_e,g_f,\eta+\frac{\pi}{2},\gamma+\frac{\pi}{2}\right)}{f_5\left(g_e,g_f,\eta,\gamma\right)}Re^2\left[\alpha\right]\right)\right]}{\sqrt{f_5\left(g_c,g_d,\eta+\frac{\pi}{2},\gamma+\frac{\pi}{2}\right)f_5\left(g_e,g_f,\eta,\gamma\right)}}, \tag{4.20}$$

onde

$$f_3\left(g_c,g_d,\eta,\gamma\right)=8e^{2(r_1+r_2)}(g_c\sin(\eta)\sin(\theta)\sin(\xi)+g_d\sin(\gamma)\cos(\theta)\cos(\xi)-1)^2, \tag{4.21}$$

$$\begin{aligned} f_4\left(g_c,g_d,\eta,\gamma\right) &= 2e^{2r_2}\left(\sin^2(\xi)\left(2g_c^2e^{2r_1}\sin^2(\eta)+(g_c\cos(\eta)+1)^2+e^{4r_1}(g_c\cos(\eta)\right.\right.\\ &\quad \left.-1)^2\right)+2e^{2r_1}\Big)+2e^{2r_1}\cos^2(\xi)\left(2g_d^2e^{2r_2}\sin^2(\gamma)+(g_d\cos(\gamma)+1)^2\right.\\ &\quad \left.+e^{4r_2}(g_d\cos(\gamma)-1)^2\right) \end{aligned} \tag{4.22}$$

e

$$\begin{aligned} f_5\left(g_e,g_f,\eta,\gamma\right) &= e^{2(r_1+r_2)}\sin^2(\xi)\left(2g_e^2\left(-2\cos(2\eta)\sinh^2(r_1)+\cosh(2r_1)+1\right)-8g_e\right.\\ &\quad \left.\times\sin(\eta)\sinh(2r_1)+4\cosh(2r_1)\right)+e^{2(r_1+r_2)}\cos^2(\xi)\left(4g_f^2\left(\cosh^2(r_2)\right.\right.\\ &\quad \left.\left.-\cos(2\gamma)\sinh^2(r_2)\right)-8g_f\sin(\gamma)\sinh(2r_2)+4\cosh(2r_2)\right)\\ &\quad +4e^{2(r_1+r_2)}. \end{aligned} \tag{4.23}$$

Ao compararmos a equação (4.20) com a equação (3.12), vemos uma quebra de simetria na forma funcional da equação da fidelidade. Na equação (3.12) as partes real e imaginária do estado são divididas pela mesma função. No atual protocolo, no entanto,

essa simetria entre as partes real e imaginária do estado é quebrada ao utilizarmos dois canais paralelos. Apesar das equações (4.22) e (4.23) possuírem termos semelhantes, a equação (4.23) possui termos a mais. Essa perda de simetria e gerada pelo fato de Bob medir apenas uma das quadraturas de campo no encerramento do protocolo.

Podemos ver que a equação (4.20) depende dos parâmetros livres θ, η, γ, g_c, g_d, g_e, g_f, ξ e do estado $|\alpha\rangle$. E para que tenhamos uma fidelidade independente do estado de entrada, é necessário que $f_3\left(g_c, g_d, \eta, \gamma\right) = f_3\left(g_e, g_f, \eta + \frac{\pi}{2}, \gamma + \frac{\pi}{2}\right) = 0$. Uma solução que satisfaz essa equação é tal que $g_d = \csc(\gamma)\sec(\theta)\sec(\xi)(1 - g_c \sin(\eta)\sin(\theta)\sin(\xi))$ e $g_f = \sec(\gamma)\sec(\theta)\sec(\xi)(1 - g_e \cos(\eta)\sin(\theta)\sin(\xi))$. Substituindo esses parâmetros de volta na equação (4.20) e realizando a maximização em função dos deslocamentos, temos que os deslocamentos que maximizam a fidelidade independente do estado de entrada são dados por

$$\begin{aligned} g_c &= \frac{\sin(\eta)\tan(\theta)\sec(\theta)\csc(\xi)\left(\csc^2(\gamma)\cosh\left(2r_2\right) - 2\sinh^2\left(r_2\right)\right)}{\sin^2(\eta)\left(\tan^2(\theta)\left(\csc^2(\gamma)\cosh\left(2r_2\right) - 2\sinh^2\left(r_2\right)\right) + 1\right) + \cos^2(\eta)\cosh\left(2r_1\right)} \\ &- \frac{\sin(\eta)\tan(\theta)\cot(\gamma)\cot(\xi)\sinh\left(2r_2\right)}{\sin^2(\eta)\left(\tan^2(\theta)\left(\csc^2(\gamma)\cosh\left(2r_2\right) - 2\sinh^2\left(r_2\right)\right) + 1\right) + \cos^2(\eta)\cosh\left(2r_1\right)} \\ &+ \frac{\cos(\eta)\sinh\left(2r_1\right)}{\sin^2(\eta)\left(\tan^2(\theta)\left(\csc^2(\gamma)\cosh\left(2r_2\right) - 2\sinh^2\left(r_2\right)\right) + 1\right) + \cos^2(\eta)\cosh\left(2r_1\right)}, \end{aligned} \tag{4.24}$$

$$\begin{aligned} g_d &= \frac{\csc(\gamma)\sec(\theta)\sin(\eta)\sin(\eta)\left(\sec(\xi) + \cot(\gamma)\sin(\theta)\tan(\theta)\sinh\left(2r_2\right)\right)}{\sin^2(\eta)\left(\tan^2(\theta)\left(\csc^2(\gamma)\cosh\left(2r_2\right) - 2\sinh^2\left(r_2\right)\right) + 1\right) + \cos^2(\eta)\cosh\left(2r_1\right)} \\ &- \frac{\csc(\gamma)\sec(\theta)\sin(\eta)\cos(\eta)\sin(\theta)\tan(\xi)\sinh\left(2r_1\right)}{\sin^2(\eta)\left(\tan^2(\theta)\left(\csc^2(\gamma)\cosh\left(2r_2\right) - 2\sinh^2\left(r_2\right)\right) + 1\right) + \cos^2(\eta)\cosh\left(2r_1\right)} \\ &+ \frac{\csc(\gamma)\sec(\theta)\cos^2(\eta)\sec(\xi)\cosh\left(2r_1\right)}{\sin^2(\eta)\left(\tan^2(\theta)\left(\csc^2(\gamma)\cosh\left(2r_2\right) - 2\sinh^2\left(r_2\right)\right) + 1\right) + \cos^2(\eta)\cosh\left(2r_1\right)}, \end{aligned} \tag{4.25}$$

$$\begin{aligned} g_e &= \frac{2\cos(\eta)\tan(\theta)\left[\sec(\theta)\csc(\xi)\left(\csc^2(\gamma) + 2\sinh^2\left(r_2\right)\right) - \cot(\gamma)\cot(\xi)\sinh\left(2r_2\right)\right]}{2\cos^2(\eta)\tan^2(\theta)\left(\csc^2(\gamma) + 2\sinh^2\left(r_2\right)\right) + \cot^2(\gamma)\left(-2\cos(2\eta)\sinh^2\left(r_1\right) + \cosh\left(2r_1\right) + 1\right)} \\ &+ \frac{2\cot^2(\gamma)\sin(\eta)\sinh\left(2r_1\right)}{2\cos^2(\eta)\tan^2(\theta)\left(\csc^2(\gamma) + 2\sinh^2\left(r_2\right)\right) + \cot^2(\gamma)\left(-2\cos(2\eta)\sinh^2\left(r_1\right) + \cosh\left(2r_1\right) + 1\right)} \end{aligned} \tag{4.26}$$

e

$$
\begin{aligned}
g_f \;=\; & \frac{\csc(\gamma)\sec(\theta)\cot(\gamma)\sec(\xi)}{2\cos^2(\eta)\tan^2(\theta)\left(\csc^2(\gamma)+2\sinh^2(r_2)\right)+\cot^2(\gamma)\left(-2\cos(2\eta)\sinh^2(r_1)+\cosh(2r_1)+1\right)} \\
& +\frac{\csc(\gamma)\sec(\theta)\cot(\gamma)\sec(\xi)\left(\cosh(2r_1)-2\cos(2\eta)\sinh^2(r_1)\right)}{2\cos^2(\eta)\tan^2(\theta)\left(\csc^2(\gamma)+2\sinh^2(r_2)\right)+\cot^2(\gamma)\left(-2\cos(2\eta)\sinh^2(r_1)+\cosh(2r_1)+1\right)} \\
& -\frac{\csc(\gamma)\sec(\theta)\cot(\gamma)\sin(2\eta)\sin(\theta)\tan(\xi)\sinh(2r_1)}{2\cos^2(\eta)\tan^2(\theta)\left(\csc^2(\gamma)+2\sinh^2(r_2)\right)+\cot^2(\gamma)\left(-2\cos(2\eta)\sinh^2(r_1)+\cosh(2r_1)+1\right)} \\
& +\frac{2\csc(\gamma)\sec(\theta)\cos^2(\eta)\sin(\theta)\tan(\theta)\sinh(2r_2)}{2\cos^2(\eta)\tan^2(\theta)\left(\csc^2(\gamma)+2\sinh^2(r_2)\right)+\cot^2(\gamma)\left(-2\cos(2\eta)\sinh^2(r_1)+\cosh(2r_1)+1\right)}.
\end{aligned}
\tag{4.27}
$$

Ao substituirmos esses parâmetros na equação (4.20), temos uma fidelidade dependente apenas dos ângulos dos divisores de feixes (DF). A maximização em termos desses ângulos é complicada e deve ser feita por meio de métodos numéricos.

Vamos, primeiro, analisar um caso particular desse problema onde fixamos os ângulos dos divisores de feixe (DF) como $\theta = \eta = \gamma = \xi = \pi/4$ e os parâmetros de compressão tal que $r_1 = r_2 = r$. Neste caso os parâmetros ótimos dos deslocamentos são $g_c = g_d = g_e = g_f = \sqrt{2}$. Esses parâmetros são os mesmos utilizados no protocolo original (Braunstein and Kimble, 1998) e pelo protocolo de multicanais em variáveis contínuas (Yonezawa et al., 2007). Ao substituí-los na eq. (4.20) temos que a fidelidade do PTVCCP é dada por $F_{cp}(\alpha, \hat{\rho}_{out}) = 1/(1+e^{-2r})$, que é exatamente igual a fidelidade do protocolo original (Braunstein and Kimble, 1998). Há alguns pontos a serem destacados desse resultado. O primeiro é que utilizando esses parâmetros nosso PTVCCP já supera o protocolo de Yonezawa et al. (2007), cuja a fidelidade é dada por $F_{seq}(\alpha, \hat{\rho}_{out}) = 1/(1+ne^{-2r})$, onde n é o número de canais. Outro ponto interessante surge ao compararmos nosso protocolo com o protocolo híbrido de Andersen and Ralph (2013). Nessa configuração a fidelidade do protocolo híbrido possuí uma eficiência de $\approx 57\%$[2], utilizando como recurso de emaranhamento 2 ebits. Usando a equação (2.31), temos que para possuirmos o recurso de 2 ebits de emaranhamento nos dois canais do PTVCCP o parâmetro de compressão de cada canal deve ser $r \approx 0.52$, de modo que para esse emaranhamento nosso protocolo com dois canais tem uma eficiência de 73%. Ou seja, superamos também o protocolo híbrido de Andersen and Ralph (2013) usando o mesmo número de canais e o mesmo recurso de emaranhamento. Um terceiro ponto a se destacar é a igualdade da expressão da fidelidade com a do protocolo original, mesmo utilizando o dobro do recurso de emaranhamento. A seguir tentaremos entender um pouco mais as causas desse último ponto, fazendo a maximização completa da fidelidade, onde agora os ângulos dos divisores de feixes são parâmetros livres.

[2]Esse protocolo utiliza estados de Bell cujo emaranhamento é definido como um ebit. Isto é, cada estado de Bell compartilhado entre Alice e Bob fornece um ebit de emaranhamento.

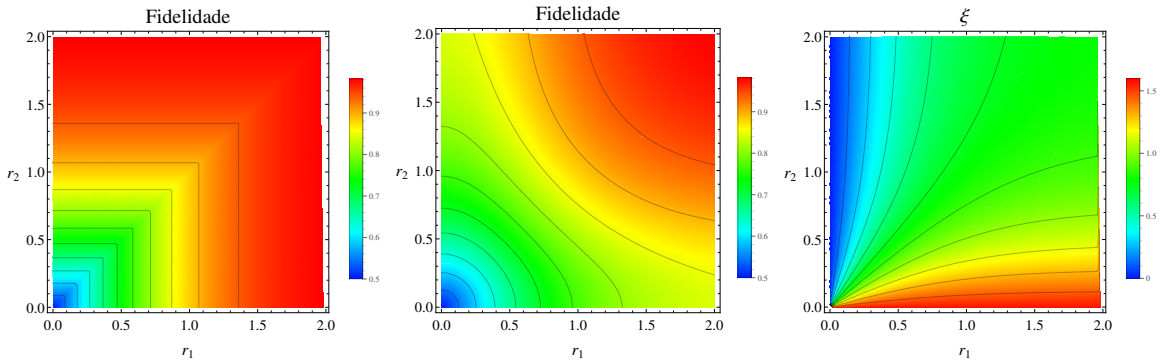


Figura 4.3: *(a) A figura mostra a fidelidade independente do estado de entrada maximizada em termos dos ângulos dos DF. Os ângulos dos DF possuem três valores distintos em três regiões distintas do gráfico. Na região onde $r_2 > r_1$, os ângulos possuem os valores de $\theta = 0$, $\gamma = \pi/4$, $\eta = \pi/4$ e $\xi = 0$. Na reta $r_2 = r_1$, os ângulos assumem os valores $\theta = \gamma = \eta = \xi = \pi/4$. Finalmente, para $r_2 < r_1$, temos $\theta = \pi/2$ $\gamma = \pi/4$, $\eta = \pi/4$ e $\xi = \pi/2$. (b) Aqui temos a fidelidade onde impomos o valor $\theta = \pi/4$, resultando nos ângulos $\gamma = \pi/4$, $\eta = \pi/4$ e ξ mostrado na figura (c).*

A figura 4.3(a) mostra a fidelidade independente do estado de entrada, equação (4.20), com os parâmetros g_c, g_d, g_e e g_f dados pelas equações (4.24-4.27) e maximizada em função dos ângulos dos divisores de feixe. A figura 4.3(a), possui três regiões distintas onde os ângulos dos divisores de feixes possuem valores diferentes. Na região onde $r_2 > r_1$ os ângulos ótimos são $\theta = 0$, $\gamma = \pi/4$, $\eta = \pi/4$ e $\xi = 0$. Na reta $r_2 = r_1$ os ângulos assumem os valores $\theta = \gamma = \eta = \xi = \pi/4$. E para $r_2 < r_1$ temos $\theta = \pi/2$ $\gamma = \pi/4$, $\eta = \pi/4$ e $\xi = \pi/2$. Um fato interessante é que os valores maximizados da fidelidade, figura 4.3(a), são sempre iguais ao valor da fidelidade do protocolo original (Braunstein and Kimble, 1998) usando-se maior parâmetro de compressão do PTVCCP, isto é, r_1 ou r_2. Ao analisarmos com mais detalhes, vemos que os dois canais só participam do protocolo quando ambos possuem o mesmo emaranhamento. Caso isso não ocorra, há uma reflexão ou transmissão total do estado em DF(θ) e DF(ξ), de modo que o estado não é divido entre os canais, sendo apenas teletransportado por apenas um canal. Ou seja, para $r_1 \neq r_2$ a melhor estratégia é utilizar um canal.

Ao forçarmos que a informação seja dividida entre os dois canais, ou seja, ao impormos $\theta = \pi/4$, a fidelidade do PTVCCP para $r_1 \neq r_2$ decai, veja figura 4.3(b), ficando abaixo da fidelidade do protocolo original (Braunstein and Kimble, 1998). Nesta situação os ângulos ótimos dos DF são dados por $\gamma = \pi/4$, $\eta = \pi/4$ e o ângulo ξ é mostrado na figura 4.3(c).

Em resumo, ao realizarmos o PTVCCP para dois canais e independente da distribuição de estados entregue a Alice, temos que as configurações ótimas para esse protocolo são as mesmas configurações do protocolo original. Ou seja, os ângulos dos DF são $\theta = \eta = \gamma = \xi = \pi/4$ resultando em ganhos $g_c = g_d = g_e = g_f = \sqrt{2}$ com parâmetros

de compressão iguais. Além disso, esta configuração ótima, resulta em uma fidelidade igual a do protocolo original Braunstein and Kimble (1998).

Podemos também proceder como no capítulo anterior e verificar o comportamento da fidelidade dependente do estado em posse de Alice. Contudo, ao fazermos isso, obtemos os mesmos resultados dispostos na figura 3.2 do capítulo anterior, com g_c, g_d, g_e e g_f fazendo os papéis dos parâmetros livres, g_v, g_u e θ do capítulo 3. Os ângulos ótimos dos DF são $\theta = \gamma = \eta = \xi = \pi/4$ e $r_1 = r_2$. Por fim, ao considerarmos os estados de Alice descritos pelas distribuições do capítulo 3, seção 3.2.2, obtemos os mesmos resultados para fidelidade dos encontrados no capítulo 3, seção 3.2.2.

Mostramos neste capítulo um PTVCCP utilizando dois canais com eficiência superior à produzida pelos protocolos de teletransporte sequencial (Yonezawa et al., 2007) e híbrido (Andersen and Ralph, 2013), supondo a mesma quantidade de recursos. Além disso, essa eficiência é a mesma do protocolo de teletransporte original (Braunstein and Kimble, 1998). Embora nosso PTVCCP não supere essa eficiência, devemos lembrar que o protocolo multicanais mais bem sucedido até agora, o protocolo híbrido, também não o faz para um número pequeno de canais. Essa igualdade de eficiência levanta uma série de questões. Por exemplo, será a eficiência do teletransporte original (Braunstein and Kimble, 1998) um limite superior ? Isto é, será que "dividirmos" (realizar a divisão de feixes) o estado em n partes e interagindo-o com n estados de vácuo não estamos introduzindo mais ruído? Se realmente o ruído introduzido pelo vácuo é ruim, o que ocorreria se invés de "dividirmos" o estado o combinássemos com outro estado? Para o teletransporte híbrido (Andersen and Ralph, 2013) é necessário um número maior de canais para que se atinja uma maior eficiência. Será que precisamos de mais canais aqui também? Se sim, esse número de canais é menor que o número de canais do protocolo híbrido? Como podemos ver, a adição de canais em paralelos levanta muitas questões que infelizmente não serão respondidas aqui, mas serão frutos de trabalhos futuros.

No próximo capítulo, daremos um uso prático para todo o nosso conhecimento adquirido até aqui sobre PTVC. Desenvolveremos um protocolo de criptografia cujo cerne é o PTVC, usando diretamente os resultados obtidos no capítulo 3.

Capítulo 5

Criptografia Quântica

Até hoje a única forma absolutamente segura através da qual duas partes (Alice e Bob) podem, ao menos teoricamente, compartilhar uma sequência secreta e aleatória de bits (chave) é dada pela criptografia quântica, cuja segurança é garantida pela validade dos postulados da mecânica quântica (Bennett and Brassard, 1984). Esta chave secreta é um importante ingrediente na implementação do protocolo de criptografia clássica conhecido como one-time-pad, que é comprovadamente seguro se apenas Bob e Alice conhecem a chave (Shannon and Weaver, 1949).

Os protocolos originais de distribuição de chave quântica (DCQ) são baseados em estados discretos (considerando por exemplo a polarização de fótons individuais), exigindo técnicas de contagem de fótons (*photon-counting techniques*) para a sua implementação (Bennett and Brassard, 1984; Gisin et al., 2002; Scarani et al., 2009). No entanto, detectores de fótons individuais não são eficientes e rápidos como fotodiodos usualmente utilizados para detectar luz (muitos fótons) (Scarani et al., 2009). Na mecânica quântica, esses estados quânticos de luz são descritos pelas quadraturas do campo eletromagnético quantizado que, como vimos anteriormente, são conhecidos como estados de variáveis contínuas (VC) devido ao espectro contínuo de suas quadraturas. A fim de explorar os sistemas de medição rápidos e eficientes para esses estados (detecção homódina ou heteródina), foram propostos vários protocolos de DCQ com base estados VC (Grosshans and Grangier, 2002; Grosshans et al., 2003; Hillery, 2000; Ralph, 1999; Reid, 2000). Todos esses protocolos são chamados protocolos de distribuição de chave quântica em variáveis contínuas (DCQVC) (Braunstein and van Loock, 2005; Weedbrook et al., 2012) e são considerados teoricamente seguros (Gottesman and Preskill, 2001; Grosshans and Cerf, 2004; Iblisdir et al., 2004; Navascués et al., 2006).

Os recursos quânticos dos primeiros protocolos DCQVC (Cerf et al., 2001; Ralph, 1999), cuja segurança era equivalente a dos protocolos DCQ discretos, eram estados comprimidos de um único modo, enviados por Alice a Bob, ou estados comprimidos de dois modos compartilhados entre eles. Nesses primeiros protocolos a chave secreta foi codificada tanto em um alfabeto binário composto de dois estados coerentes diferentes

(modulação discreta) (Ralph, 1999), como em estados coerentes com quadraturas reais e imaginárias escolhidos de uma distribuição Gaussiana (modulação contínua) (Cerf et al., 2001). Um importante desenvolvimento na DCQVC foi feito por Grosshans and Grangier (2002), onde foi mostrado que os estados coerentes são igualmente seguros para gerar uma chave secreta entre Alice e Bob caso usássemos modulação Gaussiana contínua e se as perdas na transmissão de Alice para Bob não excedesse 50%. Subsequentemente, em Silberhorn et al. (2002) foi mostrado que se Bob aceita apenas determinados resultados de medidas (pós-seleção) para gerar a chave, ou se Alice e Bob empregarem técnicas de reconciliação reversa (Grosshans et al., 2003), pode-se ultrapassar o limiar de 50% de perda. Além disso, através do emprego simultâneo das duas técnicas, pós-seleção e reconciliação reversa, obtém-se as maiores taxas de geração chave (Heid and Lütkenhaus, 2006, 2007).

A técnica de reconciliação é uma técnica de correção de erros implementada ao final do protocolo por Alice e Bob, em que eles executam um conjunto de tarefas a fim de chegar a uma sequência de bits em comum. Esse técnica é chamada direta se Alice, quem envia os estados quânticos, comunica-se classicamente com Bob, que processa seus dados usando um algoritmo pré-determinado para corrigir seus bits. A reconciliação reversa é o cenário oposto, onde Bob se comunica com Alice, que agora manipula seus dados a fim de compartilhar uma chave segura com Bob. Até o momento, não há nenhum protocolo DCQVC que é seguro para perdas de 50% na transmissão usando apenas reconciliação direta e sem pós-seleção.

Nessa capítulo, vamos mostrar o primeiro método de realizar DCQVC de maneira segura para perdas superiores a 90% na transmissão, sem recorrer a pós-seleção ou reconciliação reversa. Além de seu significado prático, este protocolo também contribui para uma compreensão fundamental do DCQVC uma vez que se baseia no uso ativo do PTVC (Braunstein and Kimble, 1998; Vaidman, 1994), abrindo caminho alternativo para compreender a segurança da DCQVC bem como diferentes rotas para futuras provas de segurança incondicional (Gottesman and Preskill, 2001).

Seguindo Gordon and Rigolin (2010) e nossos resultados obtidos no capítulo 3, a ideia principal por trás deste novo protocolo é o uso ativo dos recursos finitos de emaranhamento (compressão finita) intrinsecamente associados ao PTVC, combinado com o conhecimento do conjunto de estados coerentes com Alice para ser teletransportado para Bob (Luiz and Rigolin, 2013). Usando-se apropriadamente a informação sobre quais estados Alice vai teletransportar a Bob, conseguimos construir um protocolo de distribuição de chaves seguro, mesmo com perdas superiores a 90%, transformando a finitude do emaranhamento (finitude da compressão) em uma vantagem. De fato, o PTVC não é simplesmente utilizado como uma alternativa para o envio direto dos estados com Alice para Bob, conforme exigido pelos protocolos DCQVC citados anteriormente, em que quanto maior o emaranhamento (compressão) do canal maior a eficiência do teletransporte e subse-

quentemente mais eficiente é o protocolo de criptografia. Em nosso protocolo, no entanto, menos emaranhamento significa mais eficiência, uma vez que mostramos que para uma transmissão com perdas a quantidade de emaranhamento (compressão) que maximiza a taxa de segurança é finita e depende do nível de perda e dos estados coerentes escolhidos para codificar a chave.

5.1 Protocolo

Nessa seção descrevemos o protocolo DCQVC, procedendo da mesma maneira que nos capítulos anteriores. Iniciamos com uma análise qualitativa do protocolo, definindo um alfabeto (o qual também chamaremos de base ao longo do texto) que será teletransportado usando o PTVC. Em seguida faremos uma análise quantitativa, dando toda descrição matemática do protocolo. Faremos isso utilizando a representação de Schrödinger, expressando o PTVC nesta representação a fim de enfatizar seu papel central no protocolo DCQVC. Após essa análise quantitativa realizamos a análise de segurança do protocolo, onde mostramos sua robustez frente aos ataques mais usais.

5.1.1 Análise Qualitativa

Para o funcionamento correto dos protocolos usuais de criptografia quântica necessitamos que o estado com Alice seja transmitido a Bob sem perda de informação (ou com pouca perda). No nosso caso faremos o teletransporte deste estado usando um canal com emaranhamento finito. Para isso utilizamos o conhecimento adquirido no capítulo 3, onde mostramos como teletransportar um conjunto finito de estados com alta fidelidade mesmo com pouco emaranhamento. Aqui, Alice usará quatro estados coerentes, divididos em duas partes, $\{|\alpha\rangle, |-\alpha\rangle\}$ e $\{|i\alpha\rangle, |-i\alpha\rangle\}$, $\alpha > 0$, que chamamos de base (alfabeto) real e imaginária, respectivamente (veja figura 5.1).

Antes do início do protocolo Alice e Bob concordam com a codificação binária de seu alfabeto (Hirano et al., 2003), associando cada estado coerente com o valor do bit da chave: $\{|-\alpha\rangle, |-i\alpha\rangle\} \rightarrow 0$ e $\{|\alpha\rangle, |i\alpha\rangle\} \rightarrow 1$. Uma vez definida a codificação, em cada execução do protocolo Alice escolhe aleatoriamente entre a base real e imaginária, e em seguida escolhe de modo aleatório um dos dois estados que pertencem à base escolhida. Após essa escolha Alice procede com o PTVC. Vamos chamar o estado escolhido por Alice de $|\varphi\rangle$, que será teleportado a Bob por meio de estado comprimido de dois modos $|\psi_r\rangle$, com parâmetro de compressão r. Alice prepara o canal $|\psi_r\rangle$, ficando com um modo do estado e enviando o outro modo a Bob. A fim de encerrar a sua parte do teletransporte, Alice combina o seu modo do canal emaranhado com o estado $|\varphi\rangle$ através de um divisor de feixes com transmitância $\cos^2(\theta)$, onde θ é escolhido dependendo da base usada por Alice (veja capítulo 3 subseção 3.2.1). Após combinar os estados Alice realiza

as medidas nas quadraturas (posição e momento), informando a Bob, por comunicação clássica, o resultado das medições ($\tilde{x}_u$ e $\tilde{p}_v$). De posse das informações das medidas de

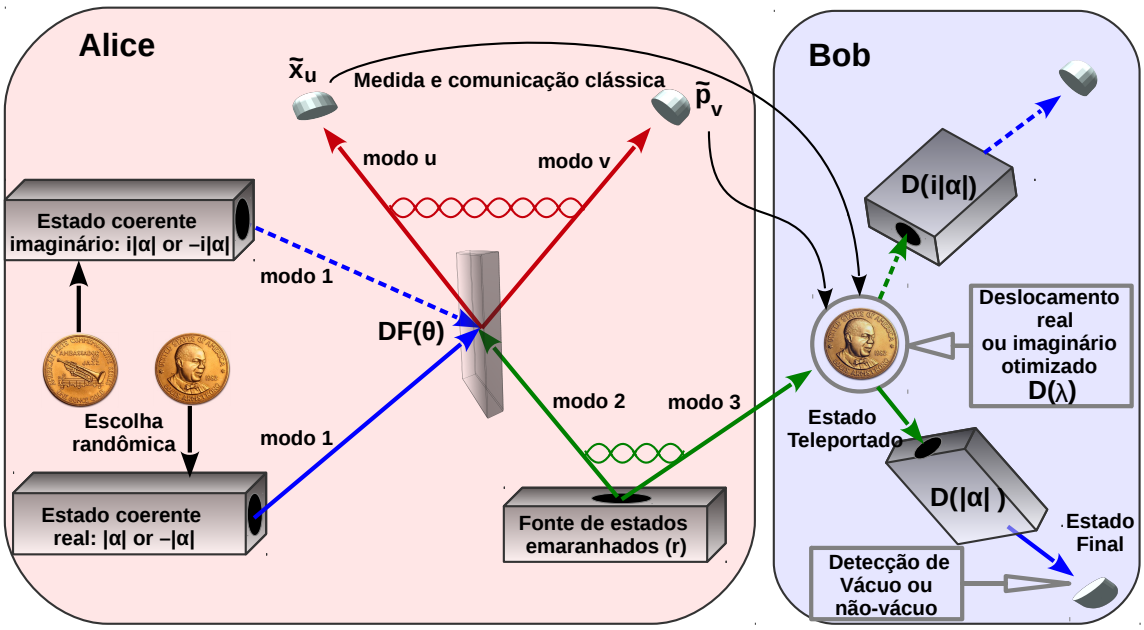


Figura 5.1: *Representação esquemática do protocolo DCQVC baseado em teletransporte. A codificação da chave binária em que Alice e Bob concordam é* $\{|-\alpha\rangle, |\alpha\rangle, |-i\alpha\rangle, |i\alpha\rangle\}=\{0,1,0,1\}$, *onde* α *é um número real.*

Alice, Bob escolhe aleatoriamente entre dois possíveis tipos de deslocamentos $\hat{D}(\lambda)$ para implementar em seu modo ($\lambda = g_u\tilde{x}_u + ig_v\tilde{p}_v$), que chamamos de deslocamentos real e imaginário. Esses diferentes tipos de deslocamentos são dados por diferentes tipos de pares de ganhos (g_u, g_v), e são otimizados no seguinte sentido. O deslocamento real (imaginário) é tal que o estado de Bob, $\hat{\rho}_B$, tenha a maior fidelidade possível com o estado escolhido por Alice se ela escolheu a base real (imaginária) e a menor fidelidade se a escolha de Alice foi a base imaginária (real). No entanto, impomos que os ganhos ótimos (g_u, g_v) independam do sinal ($\pm$) do estado coerente, dependendo somente da base escolhida.

O próximo passo do protocolo consiste em Bob realizar um novo deslocamento em seu estado (veja figura 5.1). Ele aplicará $\hat{D}(\alpha)$ em seu modo se ele previamente escolheu a base real ou $\hat{D}(i\alpha)$ se escolheu a base imaginária. O objetivo desse último deslocamento é transformar os estados $|-\alpha\rangle$ ou $|-i\alpha\rangle$ em estados de vácuo ou para mover o mais longe do vácuo os estados $|\alpha\rangle$ ou $|i\alpha\rangle$. Após o último deslocamento Bob mede a intensidade do seu modo e associa o bit 0 se ele não ver luz (estado de vácuo) ou o bit 1 se ele ver alguma luz. Note que esse passo pode ser substituído por qualquer estratégia destinada a discriminar dois estados coerentes, como por exemplo a medida das quadraturas de $\hat{\rho}_B$ usando detecção homódina.

Alice e Bob repetem o protocolo até que tenham dados suficientes para verificar se há um espião e ainda obter uma chave segura o suficiente para seus propósitos. Após Alice realizar todos os teletransportes e Bob realizar todas as medições, eles usam um canal clássico autenticado para divulgar as seguintes informações. Alice revela a Bob as bases usadas em cada execução do protocolo, mas nunca o estado. Bob revela a Alice os casos em que ele usou os valores ótimos de g_u e g_v correspondentes à base escolhida por Alice. Em seguida descartam todos os outros resultados em que as bases não coincidiram e usam parte dos dados restantes para determinar os parâmetros do canal quântico (perda e ruído) e verificar se há segurança na transmissão. Por fim, eles corrigem o erro nos dados não divulgados (fase de reconciliação) e geram uma chave secreta através de técnicas de amplificação de privacidade (Nielsen and Chuang, 2004, pg.628).

5.1.2 Análise Quantitativa

Procedemos agora com a análise quantitativa do protocolo DCQVC, desenvolvendo todo maquinário matemático necessário para o seu entendimento. O conjunto de estados que podem ser teletransportado por Alice é dado por $\{|\alpha\rangle, |-\alpha\rangle, |i\alpha\rangle$ e $|-i\alpha\rangle\}$, como já mencionado anteriormente, com $\alpha > 0$. Alice e Bob tem pleno conhecimento sobre os elementos desse conjunto, os quais são agrupados em dois alfabetos (ou base) binários: O alfabeto real $\{|\alpha\rangle, |-\alpha\rangle\}$ e o alfabeto imaginário $\{|i\alpha\rangle, |-i\alpha\rangle\}$. A codificação binária desses estado é dada pela seguinte regra: $\{|-\alpha\rangle, |-i\alpha\rangle\} \to 0$ e $\{|\alpha\rangle, |i\alpha\rangle\} \to 1$.

Alice inicia o protocolo escolhendo aleatoriamente qualquer estado do seu conjunto para enviar a Bob. Qualquer estado escolhido por Alice pode ser expresso na base da posição como

$$|\varphi\rangle = \int dx_1 \varphi(x_1)|x_1\rangle, \tag{5.1}$$

onde $\varphi(x_1) = \langle x_1|\varphi\rangle$. Em seguida, Alice prepara um canal emaranhado (comprimido) de dois modos e envia um dos modo a Bob (veja figura 5.1). O estado comprimido de dois modos compartilhado por Alice e Bob também pode ser expresso na base da posição como

$$|\psi_r\rangle = \int dx_2 dx_3 \psi_r(x_2, x_3)|x_2, x_3\rangle, \tag{5.2}$$

onde $\psi_r(x_2, x_3) = \langle x_2, x_3|\psi_r\rangle$, o modo 2 pertence a Alice, e o modo 3 a Bob (veja figura 5.1). Usando as equações (5.1) e (5.2) podemos escrever todos os modos antes do teletransporte como

$$\begin{aligned} |\Psi\rangle &= |\varphi\rangle \otimes |\psi_r\rangle, \\ &= \int dx_1 dx_2 dx_3 \varphi(x_1)\psi_r(x_2, x_3)|x_1, x_2, x_3\rangle. \end{aligned} \tag{5.3}$$

Alice continua o protocolo enviando o modo 1 e o modo 2 a um divisor de feixes (DF) com transmitância igual a $\cos^2(\theta)$. A operação realizada pelo divisor de feixes é representada pela aplicação do operador (2.82). Logo, após a aplicação do divisor de feixes podemos escrever o estado (5.3) como

$$|\Psi'\rangle = \int dx_v dx_u dx_3 \varphi(x_v \sin(\theta) + x_u \cos(\theta)) \psi_r(x_v \cos(\theta) - x_u \sin(\theta), x_3) |x_v, x_u, x_3\rangle, \quad (5.4)$$

onde $x_v = x_1 \sin(\theta) + x_2 \cos(\theta)$ e $x_u = x_1 \cos(\theta) - x_2 \sin(\theta)$. O próximo passo de Alice é realizar medidas nas quadraturas do seus modos, medindo a posição no modo u e o momento no modo v. Para realizar a medida do momento é conveniente reescrevermos o modo v na base do momento. Para isso utilizamos a transformada de Fourier, equação (2.49), de modo que após a aplicação da transformada de Fourier a equação (5.4) fica,

$$\begin{aligned} |\Psi'\rangle &= \frac{1}{\sqrt{\pi}} \int dp_v dx_v dx_u dx_3 \varphi(x_v \sin(\theta) + x_u \cos(\theta)) \psi_r(x_v \cos(\theta) - x_u \sin(\theta), x_3) \\ &\times e^{-2ix_v p_v} |p_v, x_u, x_3\rangle. \end{aligned} \quad (5.5)$$

Supondo que Alice obtenha para o momento do modo v e para a posição do modo u os valores $\tilde{p}_v$ e $\tilde{x}_u$, o estado após a medida é dado por

$$|\Psi''\rangle = \frac{\hat{P}_{\tilde{p}_v, \tilde{x}_u} |\Psi'\rangle}{\sqrt{\mathbb{P}(\tilde{p}_v, \tilde{x}_u)}}. \quad (5.6)$$

Aqui $\hat{P}_{\tilde{p}_v, \tilde{x}_u} = |\tilde{p}_v, \tilde{x}_u\rangle\langle\tilde{p}_v, \tilde{x}_u| \otimes \mathbb{1}_3$ é o projetor de von Neumann, descrevendo as medidas projetivas, $\mathbb{1}_3$ é operador identidade atuando no modo 3 e $\mathbb{p}(\tilde{p}_v, \tilde{x}_u) = tr(|\Psi'\rangle\langle\Psi'|\hat{P}_{\tilde{p}_v, \tilde{x}_u})$ é a probabilidade de medir o momento $\tilde{p}_v$ e posição $\tilde{x}_u$, com tr denotando o traço total. Usando as relações (2.47) temos que

$$|\Psi''\rangle = |\tilde{p}_v, \tilde{x}_u\rangle \otimes |\chi'\rangle, \quad (5.7)$$

onde o estado de Bob é

$$\begin{aligned} |\chi'\rangle &= \frac{1}{\sqrt{\pi \mathbb{p}(\tilde{p}_v \tilde{x}_u)}} \int dx_v dx_3 \varphi(x_v \sin(\theta) + \tilde{x}_u \cos(\theta)) \psi_r(x_v \cos(\theta) - \tilde{x}_u \sin(\theta), x_3) \\ &\times e^{-2ix_v \tilde{p}_v}. \end{aligned} \quad (5.8)$$

Na equação anterior

$$\mathbb{p}(\tilde{p}_v \tilde{x}_u) = \int dx_3 |\Psi'(\tilde{p}_v, \tilde{x}_u, x_3)|^2 \quad (5.9)$$

e

$$\begin{aligned}\Psi'(\tilde{p}_v\tilde{x}_u, x_3) &= \langle \tilde{p}_v\tilde{x}_u, x_3|\Psi'\rangle = \frac{1}{\sqrt{\pi}}\int dx_v\varphi(x_v\sin(\theta)+\tilde{x}_u\cos(\theta)) \\ &\quad \times\psi_r(x_v\cos(\theta)-\tilde{x}_u\sin(\theta), x_3)e^{-2ix_v\tilde{p}_v}, \end{aligned} \tag{5.10}$$

onde a equação (5.10) é obtida usando a equação (5.5).

Por meio de um canal clássico Alice envia a Bob os resultados das medições, permitindo a Bob deslocar as quadraturas de seus modos como se segue, $x_3 \to x_3 + g_u\tilde{x}_u$ e $p_3 \to p_3 + g_v\tilde{p}_v$. Matematicamente a aplicação do operador de deslocamento é dada pela equação (3.10). Logo, usando a equação (3.10) e realizando a mudança de variável $x_3 \to x_3 - g_u\tilde{x}_u$, o modo com Bob pode ser expresso como

$$\begin{aligned}|\chi\rangle &= \frac{e^{-ig_ug_v\tilde{x}_u\tilde{p}_v}}{\sqrt{\pi\mathbb{p}(\tilde{p}_v,\tilde{x}_u)}}\int dx_v dx_3\varphi(x_v\sin\theta+\tilde{x}_u\cos\theta)\psi_r(x_v\cos\theta-\tilde{x}_u\sin\theta, x_3-g_u\tilde{x}_u) \\ &\quad \times e^{-2i(x_v-g_vx_3)\tilde{p}_v}|x_3\rangle, \\ &= \int dx_3\left(\frac{e^{-ig_ug_v\tilde{x}_u\tilde{p}_v}}{\sqrt{\pi\mathbb{p}(\tilde{p}_v,\tilde{x}_u)}}\int dx_v\varphi(x_v\sin\theta+\tilde{x}_u\cos\theta)\psi_r(x_v\cos\theta-\tilde{x}_u\sin\theta, x_3-g_u\tilde{x}_u)\right. \\ &\quad \left.\times e^{-2i(x_v-g_vx_3)\tilde{p}_v}\right)|x_3\rangle, \\ &= \int dx_3\chi(x_3)|x_3\rangle. \end{aligned} \tag{5.11}$$

Note que ao escrevermos o estado a ser teletransportado por Alice de forma genérica obtivemos o mesmo resultado para o estado final de Bob do capítulo 3. Após o fim do teletransporte do estado, Bob deve realizar um deslocamento $\hat{D}(\alpha)$ (caso tenha escolhido o alfabeto real). Porém, antes de prosseguir com o protocolo de DCQVC devemos verificar o quão próximo o estado final de Bob está do estado entrada. Para isso faremos uso da fidelidade. Assumindo que o estado coerente pertença ao alfabeto real $\{|\alpha\rangle, |-\alpha\rangle\}$ e usando as equações (2.28), (2.35) e (2.66) temos que a fidelidade fica,

$$F(|\varphi\rangle, |\chi\rangle) = h_1(r,\theta)\exp\left[f_1(\tilde{p}_v\tilde{x}_u, g_v, g_u, r, \theta) + 2\alpha\tilde{x}_u f_2(g_u, r, \theta) + \alpha^2 f_3(r,\theta)\right], \tag{5.12}$$

onde

$$h_1(r,\theta) = \sqrt{1-\cos^2(2\theta)\tanh^2(r)}, \tag{5.13}$$

$$
\begin{aligned}
f_1(\tilde{p}_v\tilde{x}_u, g_v, g_u, r, \theta) &= \left\{\left[g_u^2\tilde{x}_u^2 - g_v^2\tilde{p}_v^2\right]\cos(2\theta)\tanh(r) + 4g_u\tilde{x}_u^2\sin(\theta) + 4g_v\tilde{p}_v^2\cos(\theta)\right\} \\
&\quad \times \tanh(r) + \tilde{x}_u^2\left[-g_u^2 + \frac{2}{\cosh^2(r) - \cos(2\theta)\sinh^2(r)} - 2\right] \\
&\quad + \tilde{p}_v^2\left[-g_v^2 + \frac{2}{\cosh^2(r) + \cos(2\theta)\sinh^2(r)} - 2\right], \qquad (5.14)
\end{aligned}
$$

$$
\begin{aligned}
f_2(g_u, r, \theta) &= g_u - \left\{g_u\cos(2\theta)\tanh r + 2[1 + g_u\cos\theta]\sin\theta\right\}\tanh r \\
&\quad + 2\left(\frac{1}{\cos(2\theta)\sinh^2 r - \cosh^2 r} + 1\right)\cos\theta \qquad (5.15)
\end{aligned}
$$

e

$$
f_3(r, \theta) = -\frac{\left\{\cosh r - [\tanh r\cos(2\theta) + \sin(2\theta)]\sinh r\right\}^2}{\cosh^2 r - \cos(2\theta)\sinh^2 r}. \qquad (5.16)
$$

Queremos que a fidelidade independa do sinal do estado coerente α e para isso impomos que $f_2(g_u, r, \theta) = 0$. Com isso temos que o valor do parâmetro g_u vale

$$
g_u(r, \theta) = \frac{\sinh(2r)\sin(\theta)}{\cosh^2(r) - \cos(2\theta)\sinh^2(r)}. \qquad (5.17)
$$

Substituindo a equação acima na equação da fidelidade (5.12) e maximizando-a na variável g_v obtemos

$$
g_v(r, \theta) = \frac{2\coth(r)\cos(\theta)}{\coth^2(r) + \cos(2\theta)}. \qquad (5.18)
$$

Um ponto interessante a se notar é que ao considerarmos uma distribuição de estados sobre a reta real e calcularmos a fidelidade média, a expressão para g_u é a mesma da equação (5.17). Logo, ao impormos a independência do sinal do estado, a solução para o parâmetro g_u para dois estados é a mesma quando consideramos uma distribuição de estados reais. Inserindo as equações (5.17) e (5.18) na fidelidade, equação (5.12), temos

$$
\begin{aligned}
F^{re}(r, \theta) &= \sqrt{1 - \cos^2(2\theta)\tanh^4(r)} \\
&\quad \times \exp\left\{\frac{-\alpha^2\left\{\cosh(r) - \sinh(r)[\cos(2\theta)\tanh(r) + \sin(2\theta)]\right\}^2}{\cosh^2(r) - \cos(2\theta)\sinh^2(r)}\right\}, \qquad (5.19)
\end{aligned}
$$

onde usamos o sobrescrito "re" para lembrar que esta fidelidade é para o alfabeto real. Além disso, é importante notar que a expressão da fidelidade, bem como para g_v e g_u, não dependem dos resultados das medidas $\tilde{x}_u$ e $\tilde{p}_v$ obtidas por Alice. Esta é uma das razões que fazem esse protocolo DCQVC ter uma alta taxa de eficiência sem a pós-seleção de todos os possíveis resultados das medidas de Alice.

Considerando como entrada o alfabeto imaginário, ou seja, estados $|i\alpha\rangle$ ou $|-i\alpha\rangle$, os papéis de g_u e g_v ótimos são invertidos. Como também é visto na análise da fidelidade média para uma distribuição na reta imaginária, capítulo 3, seção 3.2.2. Para obter uma solução para a fidelidade independente do sinal do estado coerente procedemos da mesma maneira que no alfabeto real, o que nos leva às mesmas expressões do caso real para g_u e g_v. Substituindo essas expressões na fidelidade temos

$$\begin{aligned} F^{im}(r,\theta) &= \sqrt{1-\cos^2(2\theta)\tanh^4(r)} \\ &\quad \times \exp\left\{\frac{-\alpha^2\{\cosh r+\sinh r[\cos(2\theta)\tanh r-\sin(2\theta)]\}^2}{\cosh^2 r+\cos(2\theta)\sinh^2 r}\right\}. \end{aligned} \tag{5.20}$$

Comparando ambas expressões da fidelidade vemos que

$$F^{re}(r,\theta) = F^{im}(r,\pi/2-\theta). \tag{5.21}$$

Com isso, a diferença entre as fidelidade é dada pela escolha do ângulo do divisor de feixes, assim como visto na análise das distribuições puramente reais ou imaginárias (capítulo 3, seção 3.2.2).

Para otimizar as fidelidades, necessitamos agora determinar r e θ. Desejamos r e θ tal que se Alice escolhe o alfabeto real e Bob supõe que Alice escolheu o alfabeto real, $F^{re}(r,\theta)$ seja máxima e $F^{im}(r,\theta)$ seja mínima. Isso é conseguido ao maximizar a função

$$\Pi^{re}(r,\theta) = F^{re}(r,\theta)\left[1-F^{im}(r,\theta)\right]. \tag{5.22}$$

Não é possível obter uma expressão analítica que maximize a função acima em termos de r e θ. Desse modo, a maximização é feita numericamente uma vez que α seja especificado. Os dados da maximização estão na figura 5.2. Nela podemos ver que quando Bob e Alice concordam no alfabeto transmitido a fidelidade tende a um (linha preta com círculos pretos) e quando eles discordam a fidelidade tende a zero (linha vermelha com quadrados vermelhos), mostrando uma clara distinção entre as duas possibilidades.

Os parâmetros ótimos caso Alice escolha o alfabeto imaginário e Bob suponha que Alice escolheu o alfabeto imaginário é obtido impondo que F^{re} seja mínimo e F^{im} seja máximo. Isso é obtido através da maximização da função:

$$\Pi^{im}(r,\theta) = F^{im}(r,\theta)\left[1-F^{re}(r,\theta)\right] = \Pi^{re}(r,\pi/2-\theta). \tag{5.23}$$

Pela última igualdade, podemos ver que o ângulo do divisor de feixes θ ótimo para o alfabeto imaginário é obtido a partir do ângulo ótimo para o alfabeto real subtraindo-o de $\pi/2$. Dessa forma, as relações entre os melhores ajustes considerando o alfabeto real

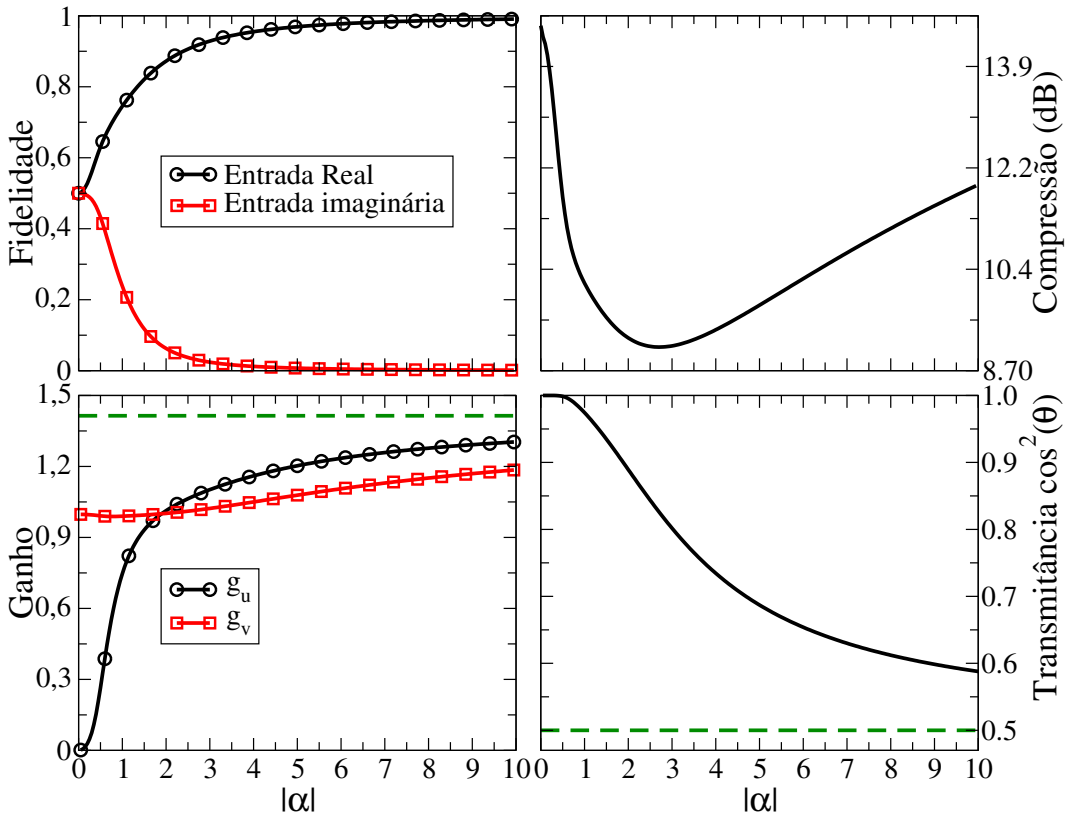


Figura 5.2: *Parâmetros otimizados resultando em uma maior (menor) fidelidade para o teletransporte de um estado coerente real (imaginário). As configurações ótimas para a maior (menor) fidelidade para o estado imaginário (real) de entrada são obtidas a partir dos parâmetros do estado real permutando g_v com g_u e mudando θ por $\pi/2 - \theta$. O parâmetro de compressão permanece inalterado. As curvas tracejadas dão as configurações do PTVC original Braunstein and Kimble (1998).*

ou imaginário como entrada são as seguintes:

$$\theta^{re} = \pi/2 - \theta^{im}, \tag{5.24}$$

$$g_v^{re} = g_u^{im}, \tag{5.25}$$

$$g_u^{re} = g_v^{im}, \tag{5.26}$$

$$r^{re} = r^{im}. \tag{5.27}$$

Conseguimos, assim, um conjunto de parâmetros que torna a implementação do protocolo factível com alto grau de diferenciabilidade entre os alfabetos.

Retornando ao protocolo de DCQVC, o estado de Bob após o término do PTVC é dado pela equação (5.11). Bob então deve executar o último passo do protocolo DCQVC implementando outro deslocamento, que depende da escolha do alfabeto (real ou imaginário) feita previamente por ele. Caso Bob tenha feita a escolha do alfabeto real ele deve aplicar o deslocamento $\hat{D}(\alpha)$ em seu modo. Caso a escolha prévia feita por ele tenha sido pelo alfabeto imaginário Bob deve aplicar o deslocamento $\hat{D}(i\alpha)$. O objetivo desse

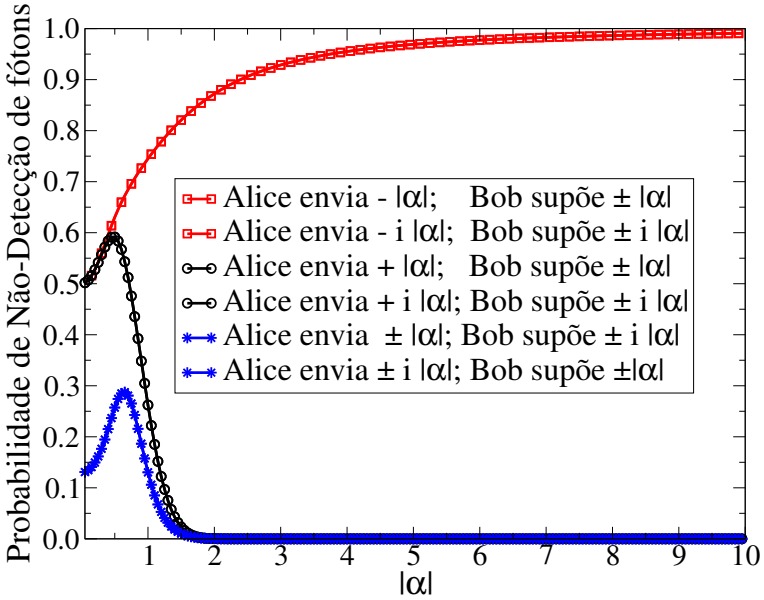


Figura 5.3: *Probabilidade de Bob detectar o estado de vácuo ao final do protocolo se Alice e Bob usarem as configurações ótimas dadas pela Fig. 5.2. A primeira curva (de cima para baixo) é Q_0^B calculada para os seguintes parâmetros: estado de entrada com Alice $= |-\alpha\rangle$ e r^{re}, θ^{re}, $\lambda = g_u^{re}\tilde{x}_u + ig_v^{re}\tilde{p}_v$, $\gamma = \alpha$. A segunda curva é Q_0^B para os parâmetros $|-i\alpha\rangle$, r^{im}, θ^{im}, $\lambda = g_u^{im}\tilde{x}_u + ig_v^{im}\tilde{p}_v$, $\gamma = i\alpha$. A terceira curva é Q_0^B para o estado de entrada de Alice $= |\alpha\rangle$ e r^{re}, θ^{re}, $\lambda = g_u^{re}\tilde{x}_u + ig_v^{re}\tilde{p}_v$, $\gamma = \alpha$. Para a quarta curva os parâmetros são $|i\alpha\rangle$, r^{im}, θ^{im}, $\lambda = g_u^{im}\tilde{x}_u + ig_v^{im}\tilde{p}_v$, $\gamma = i\alpha$. A quinta curva é a média de Q_0^B para os parâmetros $|\pm\alpha\rangle$, r^{re}, θ^{re}, $\lambda = g_u^{im}\tilde{x}_u + ig_v^{im}\tilde{p}_v$, $\gamma = i\alpha$. A sexta curva é a média de Q_0^B para os parâmetros $|\pm i\alpha\rangle$, θ^{im}, r^{im}, $\lambda = g_u^{re}\tilde{x}_u + ig_v^{re}\tilde{p}_v$, $\gamma = \alpha$. Sempre que Bob assume incorretamente a base (alfabeto) utilizada por Alice, ele não pode discernir entre as duas entradas possíveis (curvas estrelas/azuis).*

deslocamento é transformar os estados $|-\alpha\rangle$ ou $|-i\alpha\rangle$ em estados de vácuo e levar os estados $|\alpha\rangle$ ou $|i\alpha\rangle$ para longe do estado de vácuo. Note que o estado de Bob estará muito perto de um desses quatro estados somente se a "condição de correspondência" ocorrer, ou seja, se Alice teletransportar um estado real (imaginário) e Bob usar as configurações ideais presumindo que o estado de entrada de Alice seja real (imaginário).

Matematicamente o estado de Bob após esse último deslocamento é dado por

$$|\tilde{\chi}\rangle = \hat{D}(\gamma)|\chi\rangle, \tag{5.28}$$

onde $\gamma = \alpha$ ou $\gamma = i\alpha$. Logo, a probabilidade de Bob detectar o estado de vácuo é

$$Q_0^B = |\langle 0|\tilde{\chi}\rangle|^2 = |\langle -\gamma|\chi\rangle|^2 = \left|\int dx_3 \varphi^*_{-\gamma}(x_3)\chi(x_3)\right|^2, \tag{5.29}$$

onde usamos que $\hat{D}(\gamma) = \hat{D}^\dagger(-\gamma)$ e $\langle 0|\hat{D}(\gamma) = \langle -\gamma|$. Na equação (5.29), $\varphi^*_{-\gamma}(x_3)$ é o complexo conjugado da equação (2.66), com o subíndice $-\gamma$ nos lembrarmos a quem o kernel do estado coerente $\varphi(x_3)$ se refere, e $\chi(x_3)$ é dado pela equação (2.28).

Na figura 5.3 temos o gráfico de Q_0^B para todas as possíveis combinações do estado de entrada de Alice e dos deslocamentos de Bob para quando ambos escolhem o mesmo alfabeto (as quatro primeiras curvas de cima para baixo). A quinta e sexta curva são a média de Q_0^B sobre todas as possíveis medidas de Alice, $\tilde{x}_u$ e $\tilde{p}_v$, ponderada pela probabilidade da medida de Alice resultar $\tilde{x}_u$ e $\tilde{p}_v$ (eq. 5.9),

$$q_0^B = \int d\tilde{p}_v d\tilde{x}_u \mathbb{p}(\tilde{p}_v, \tilde{x}_u) Q_0^B(\tilde{p}_v, \tilde{x}_u). \tag{5.30}$$

A média é necessária sempre que não houver condição de correspondência, pois nesse caso Q_0^B dependerá de $\tilde{x}_u$ e $\tilde{p}_v$. A figura 5.3 nos mostra que quando a condição de correspondência ocorre, Bob pode discernir entre as duas entradas possíveis. No entanto, quando não há condição de correspondência, Bob não consegue distinguir os estados.

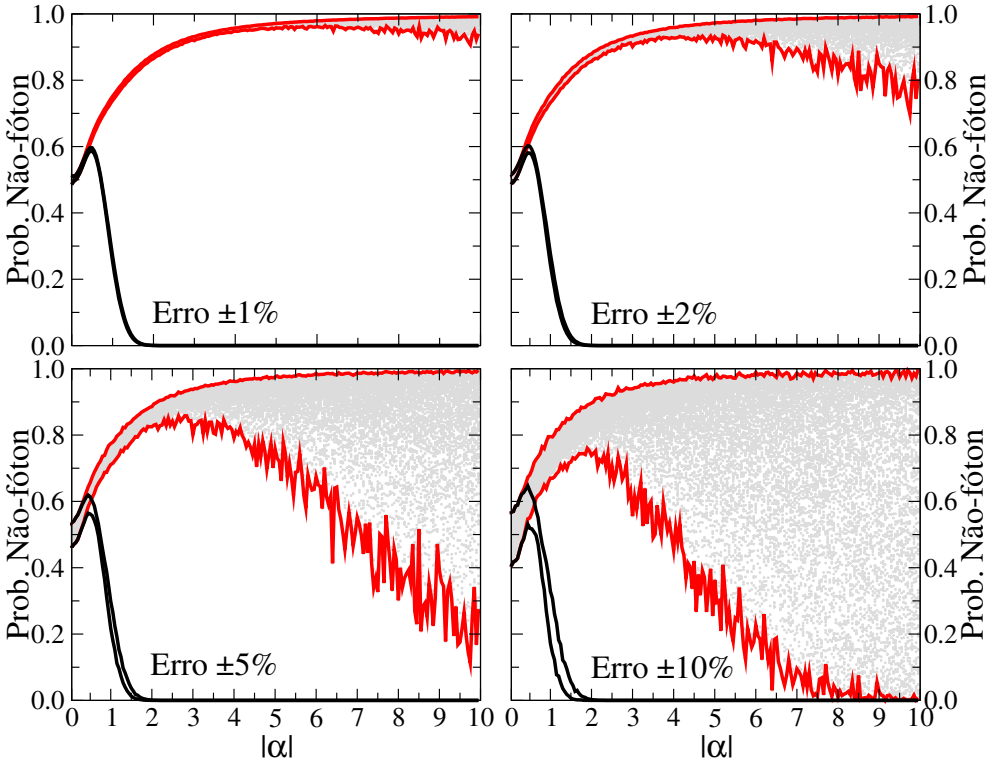


Figura 5.4: *Para cada valor de α realizamos* 100 *implementações de flutuações aleatórias no estado de entrada e nos valores ótimos r, θ, g_v, g_u e γ. Supomos que Alice envia o alfabeto (base) real a Bob, que escolhe também o alfabeto real. Resultados similares são encontrados supondo o alfabeto imaginário, com a condição de correspondência. A curva vermelha conecta o máximo e o mínimo valor de q_0^B devido às flutuações, supondo que Alice tenha enviado um estado real negativo. Os pontos cinzas entre as curvas vermelha representam q_0^B a cada realização. As curvas pretas têm o mesmo significado das curvas vermelhas porém supondo que Alice envia o estado real positivo.*

Nós também testamos a robustez das configurações ideais por flutuações aleatórias em seus valores ótimos. Consideramos flutuações nos parâmetros ótimos independentes, ou seja, tanto o estado de entrada quanto os parâmetros do sistema estão su-

jeitos a variações aleatórias independentes. A figura 5.4 mostra que os parâmetros ótimos são muito robustos, suportando flutuações de $\pm 2\%$ para valores pequenos e grandes de α. Para valores pequenos de α flutuações de $\pm 10\%$ ainda são toleradas.

Após realizar o protocolo n vezes, ao final da enésima detecção Bob divulga a base escolhida por ele em cada teletransporte através de um canal clássico. Alice realiza o mesmo procedimento revelando a base escolhida por ela. Pela figura 5.3, vemos que quando há coincidência das escolhas Bob consegue distinguir perfeitamente os estados. Desse modo, Bob e Alice descartam os estados onde não há coincidência nos alfabetos utilizados e aplicam a reconciliação de informação para corrigirem os erros e a amplificação de privacidade para maximizar a incerteza da provável espiã (Eva) sobre a chave, encerrando assim o protocolo.

Vale destacar aqui que esse protocolo usa diretamente os resultados obtidos no capítulo 3, mostrando que a análise sistemática de um problema pode resultar em aplicações práticas. Como todo protocolo de criptografia, esse protocolo ainda deve passar pelo crivo dos ataques conhecidos. Na próxima seção iremos realizar a análise de segurança do protocolo contra um dos ataques incoerentes (ou individuais) mais poderosos, o ataque de divisor de feixes (beam splitter attacks).

5.1.3 Análise de segurança

Desejamos, agora, investigar a segurança do atual protocolo frente ao ataque de divisor de feixes (ADF). No ADF a espiã (Eva) insere um DF com transmitância η, $0 \leq \eta \leq 1$, durante a transmissão do modo emaranhado de Bob (modo 3 na figura 5.1). Nesse ataque Bob irá receber um sinal com intensidade η e Eva irá receber o resto do sinal. Com sua parte do sinal Eva procede como Bob, a fim de extrair informações sobre a chave.

Alice pode enviar o modo de Bob antes ou depois de realizar suas operações. Iremos considerar que Alice realiza todas as operações e depois envia a Bob o modo 3. Desse modo, o estado enviado é descrito pela equação (5.8). Eva interfere no envio desse estado, inserindo um divisor de feixes no canal. A operação do divisor de feixes é descrita pela equação (2.82). Portanto, o estado enviado por Alice após a interferência de Eva é descrito por:

$$\begin{aligned} |\Omega\rangle &= \hat{B}_{34}(\eta)|\chi'\rangle_3|0\rangle_4 = \int dx_3 dx_4 \chi'(x_3)\varphi_0(x_4)\left|\sqrt{\eta}x_3 - \sqrt{1-\eta}x_4, \sqrt{1-\eta}x_3 + \sqrt{\eta}x_4\right\rangle, \\ &= \int dx_3 dx_4 \chi'(\sqrt{\eta}x_3 + \sqrt{1-\eta}x_4)\varphi_0(\sqrt{\eta}x_4 - \sqrt{1-\eta}x_3)|x_3, x_4\rangle, \end{aligned} \tag{5.31}$$

onde φ_0 é dado pela equação (2.66) com $\alpha = 0$. A última igualdade é obtida realizando uma mudança de variáveis, $x_3 \to \sqrt{\eta}x_3 + \sqrt{1-\eta}x_4$ e $x_4 \to \sqrt{\eta}x_4 - \sqrt{1-\eta}x_3$. O estado de Bob após a aplicação do DF é obtida pela aplicação do traço parcial sobre o estado

$\rho_{BE} = |\Omega\rangle\langle\Omega|$, em relação ao modo de Eva, $\rho'_B = tr_E(\rho_{BE})$. Logo, na base da posição o estado de Bob é dado por

$$\rho'_B = \int dx_4 \langle x_4|\rho_{BE}|x_4\rangle = \int dx_3 dx'_3 \rho'_B(x_3, x'_3)|x_3\rangle\langle x'_3|, \tag{5.32}$$

onde

$$\begin{aligned}\rho'_B(x_3, x'_3) &= \int dx_4 \chi'(\sqrt{\eta}x_3 + \sqrt{1-\eta}x_4)\chi'^*(\sqrt{\eta}x'_3 + \sqrt{1-\eta}x_4)\varphi_0(\sqrt{\eta}x_4 - \sqrt{1-\eta}x_3) \\ &\times\varphi_0^*(\sqrt{\eta}x_4 - \sqrt{1-\eta}x'_3).\end{aligned} \tag{5.33}$$

Note que o estado de Eva é $\rho'_E = tr_B(\rho_{BE})$, que é obtido da equação (5.33) simplesmente trocando $\eta \to 1-\eta$.

Usando o estado ρ'_B (ρ'_E) Bob (Eva) prossegue com o protocolo de DCQVC, realizando um deslocamento λ em seu modo que depende das medidas realizadas por Alice e da escolha do alfabeto. Bob então realiza o deslocamento λ, supondo que Alice escolheu o alfabeto real ou imaginário, encerando assim o PTVC. Após o término do PTVC o estado de Bob é $\rho_B = \hat{D}(\lambda)\rho'_B\hat{D}^\dagger(\lambda)$. Em seguida, Bob implementa o último deslocamento $\hat{D}(\gamma)$, que depende da escolha do alfabeto usado por Bob.

Após o último deslocamento a probabilidade de que Bob detecte o estado de vácuo (não observe fótons) é

$$\begin{aligned}Q_0^B(\tilde{p}_v, \tilde{x}_u) &= tr[|0\rangle\langle 0|\,\hat{D}(\gamma)\rho_B\hat{D}^\dagger(\gamma)] \\ &= \langle -\lambda-\gamma|\rho'_B|-\lambda-\gamma\rangle,\end{aligned} \tag{5.34}$$

onde explicitamos que Q_0^B depende dos resultados das medidas feitas por Alice caso $\eta \neq 1$, ou seja, quando temos perda no canal. Na base da posição a probabilidade pode ser escrita como

$$Q_0^B(\tilde{p}_v, \tilde{x}_u) = \int dx_3 dx'_3 \varphi^*_{-\lambda-\gamma}(x_3)\rho'_B(x_3, x'_3)\varphi_{-\lambda-\gamma}(x'_3). \tag{5.35}$$

A probabilidade média de Bob medir o vácuo, isto é, a probabilidade média sobre todas as possíveis medidas de Alice (ou seja, sem pós-seleção) é

$$q_0^B = \int d\tilde{p}_v d\tilde{x}_u \mathbb{p}(\tilde{p}_v, \tilde{x}_u) Q_0^B(\tilde{p}_v, \tilde{x}_u). \tag{5.36}$$

Na figura 5.5 temos a probabilidade, q_0^B, de Bob detectar o estado de vácuo com perda no envio do sinal. Ao compararmos a figura 5.5 com a figura 5.3, percebemos que a intervenção de Eva faz com que a probabilidade de Bob medir o vácuo diminua, fazendo com que ele não consiga distinguir perfeitamente os dois estados. Na figura 5.5

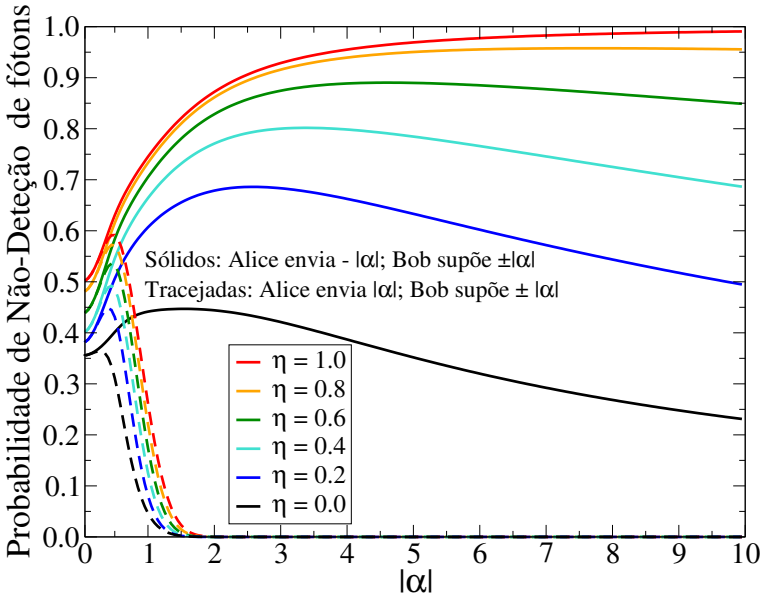


Figura 5.5: *Probabilidade q_0^B de detectar o estado de vácuo para vários valores de perda do sinal $(1-\eta)$, que aumenta (η diminui) de cima para baixo. Os outros parâmetros usados para calcular q_0^B são, r, θ, g_v, g_u, e γ, onde os valores ótimos são dados quando ocorre a condição de correspondência. O parâmetro restante, estado de entrada de Alice, foi definido como $-\alpha$ (linhas sólidas) e α (linhas tracejadas).*

podemos ver claramente que a medida que Bob perde sinal para Eva (η diminui) a probabilidade decai. Quando Bob perde todo o sinal (curva preta) a probabilidade de ele medir o vácuo é de aproximadamente 23% para α grande.

Taxa de chave segura

A taxa de chave segura para a reconciliação direta (Grosshans and Grangier, 2002) gerada por Alice e Bob considerando um ataque de DF é

$$K = \max\{0, \beta I_{AB} - I_{AE}\} = \max\{0, \Delta I\}, \tag{5.37}$$

onde β é a eficiência de reconciliação e depende do software de reconciliação aplicado. Para a codificação binária, que é usada aqui, temos $\beta \approx 80\%$ (Leverrier and Grangier, 2009, 2011). I_{AB} é a informação mútua entre Alice e Bob e I_{AE} é a informação mútua entre Alice e Eva. A taxa de chave segura mede a segurança do protocolo, sendo que esse é considerado seguro se $\beta I_{AB} > I_{AE}$. Dado que o presente protocolo e o ataque de DF são simétricos em relação aos alfabetos reais e imaginários, para essa análise de segurança consideramos apenas o caso em que Alice e Bob usaram o alfabeto real.

Sejam X e Y duas variáveis discretas binárias, cujos possíveis valores são $x = 0, 1$ e para Y são $y = 0, 1$. Se associarmos a variável X a Alice, que adotou a convenção

$\{-|\alpha\rangle, |\alpha\rangle\} = \{0, 1\}$ temos

$$P_X(0) = P_X(1) = 1/2, \tag{5.38}$$

onde $P_X(x)$ é a distribuição de probabilidade associado a X. Isso significa que Alice escolhe aleatoriamente entre o estado coerente positivo e negativo para cada rodada do protocolo.

Se associarmos a variável Y a Bob, podemos definir a probabilidade condicional de Bob atribuir o valor de y para sua variável se Alice escolhe o valor x como $P_{Y|X}(y, x)$. Para o nosso protocolo as quatro probabilidades condicionais são

$$\begin{aligned} P_{Y|X}(0|0) &= q_0^B(-\alpha), & (5.39)\\ P_{Y|X}(1|0) &= 1 - q_0^B(-\alpha), & (5.40)\\ P_{Y|X}(0|1) &= q_0^B(\alpha), & (5.41)\\ P_{Y|X}(1|1) &= 1 - q_0^B(\alpha), & (5.42) \end{aligned}$$

onde q_0^B é a probabilidade de Bob detectar o estado de vácuo dado pela equação (5.36). Se definirmos

$$q_1^B(\alpha) = 1 - q_0^B(\alpha), \tag{5.43}$$

onde q_1^B é a probabilidade de detectar luz, temos

$$\begin{aligned} P_{Y|X}(0|0) &= q_0^B(-\alpha), & (5.44)\\ P_{Y|X}(1|0) &= 1 - q_0^B(-\alpha), & (5.45)\\ P_{Y|X}(0|1) &= 1 - q_1^B(\alpha), & (5.46)\\ P_{Y|X}(1|1) &= q_1^B(\alpha). & (5.47) \end{aligned}$$

Note que escrevemos explicitamente a dependência de q_j^B, $j = 0, 1$, com o estado teletransportado por Alice para nos lembrar que devemos calculá-lo usando o sinal apropriado de α.

Podemos entender as probabilidades condicionais anteriores da seguinte forma. Se Alice teletransporta o estado $|-\alpha\rangle$ (bit 0) e Bob desloca o seu modo em α, ele irá detectar o estado de vácuo após o deslocamento final e atribuir corretamente o bit 0 com probabilidade quantificada por $P_{Y|X}(0|0) = q_0^B(-\alpha)$. Bob pode cometer um erro e não detectar o estado de vácuo atribuindo erroneamente o bit 1. Por essa razão, temos $P_{Y|X}(1|0) = 1 - q_0^B(-\alpha)$. Da mesma forma, se Alice teletransporta o estado $|\alpha\rangle$ (bit 1) e Bob desloca seu modo de α, Bob não irá detectar o estado de vácuo e irá atribuir corretamente o bit 1 com probabilidade $1 - q_0^B(\alpha)$ o que implica em $P_{Y|X}(1|1) = 1 - q_0^B(\alpha)$. Caso Bob cometa um erro e obtenha o estado de vácuo essa ação é quantificada pela

probabilidade condicional $P_{Y|X}(0|1) = q_0^B(\alpha)$.

Uma vez que a probabilidade condicional está relacionada com a distribuição de uma probabilidade conjunta $P_{XY}(x, y)$ pela regra $P_{XY}(x, y) = P_X(x)P_{Y|X}(y|x)$ temos

$$P_{XY}(0,0) = q_0^B(-\alpha)/2, \tag{5.48}$$
$$P_{XY}(0,1) = \left[1 - q_0^B(-\alpha)\right]/2, \tag{5.49}$$
$$P_{XY}(1,0) = \left[1 - q_1^B(\alpha)\right]/2, \tag{5.50}$$
$$P_{XY}(1,1) = q_1^B(\alpha)/2. \tag{5.51}$$

Usando que $P_Y(y) = \sum_x P_{XY}(x, y)$, temos

$$P_Y(0) = \left[1 + q_0^B(-\alpha) - q_1^B(\alpha)\right]/2, \tag{5.52}$$
$$P_Y(1) = \left[1 + q_1^B(\alpha) - q_0^B(-\alpha)\right]/2. \tag{5.53}$$

De posse dessas probabilidades podemos calcular a informação mútua, equação (1.4), entre Alice e Bob

$$I_{AB} = \sum_{x=0}^{1}\sum_{y=0}^{1} P_{X,Y}(x, y) \log_2 \left[\frac{P_{XY}(x, y)}{P_X(x)P_Y(y)}\right]. \tag{5.54}$$

Portanto, substituindo as equações (5.38) e (5.48-5.53) na informação mútua temos

$$\begin{aligned} I_{AB} \;=\; & 1 + [q_0^B(-\alpha)\log_2 q_0^B(-\alpha) + (1 - q_0^B(-\alpha))\log_2(1 - q_0^B(-\alpha))q_1^B \log_2 q_1^B(\alpha) \\ & +(1 - q_1^B(\alpha))\log_2(1 - q_1^B(\alpha)) - (1 + q_0^B(-\alpha) - q_1^B(\alpha))\log_2(1 + q_0^B(-\alpha) \\ & -q_1^B(\alpha)) - (1 + q_1^B(\alpha) - q_0^B(-\alpha))\log_2(1 + q_1^B(\alpha) - q_0^B(-\alpha))]/2. \end{aligned} \tag{5.55}$$

Note que I_{AB} também depende de r, θ, g_v, g_u e η. A fim de obter I_{AE} nós simplesmente substituímos η por $1 - \eta$ na expressão (5.55), uma vez que $q_j^B \to q_j^E$ se $\eta \to 1 - \eta$.

Usando a equação (5.55) e a equivalente para I_{AE} nós podemos calcular a taxa de chave segura (secure key rate) K (equação 5.37). Na figura 5.6 nós mostramos ΔI para diversos valores de η supondo a condição de concordância do alfabeto real entre Alice e Bob e empregando os parâmetros ótimos de r, θ, g_v e g_u mostrados na figura 5.2. A figura 5.6 mostra que é possível escolher um valor de α tal que, para $\beta = 0.8$ e 90% de perda obtemos $K \approx 0.03$. Esse valor deve ser comparado com protocolos sem o excesso de ruído em Silberhorn et al. (2002) e Lorenz et al. (2004), onde usando uma reconciliação direta perfeita ($\beta = 1$) e considerado pós-seleção eles obtiveram $K = 0.007$ a 75% de perda, e com o protocolo em Heid and Lütkenhaus (2006, 2007), onde acima de 80% de perda não é possível extrair a chave secreta via reconciliação direta. Em outras palavras, podemos melhorar a taxa da chave em cerca de uma ordem de grandeza supondo mais

perda. E para obter esse enorme ganho necessitamos de um parâmetro de compressão de cerca de ≈ 10 dB.

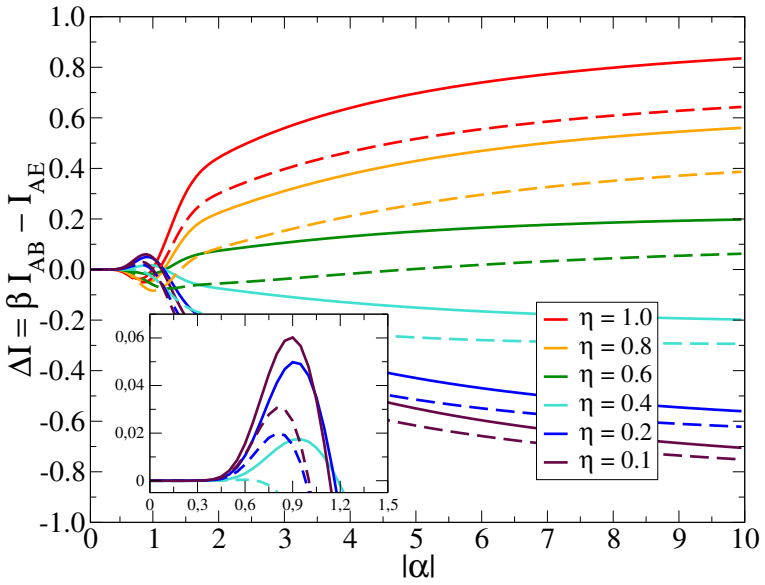


Figura 5.6: *Todos os gráficos: Curvas sólidas significam $\beta = 1.0$, curvas tracejadas $\beta = 0.8$ e todas as curvas possuem regiões com valores positivos. Gráfico principal: Para grandes valores de $|\alpha|$ temos de cima para baixo aumento (diminuição) da perda (η). Gráfico interno: $\eta = 0.1$ para o maior pico sólido e tracejado enquanto $\eta = 0.4$ para o menor pico sólido e tracejado.*

Note que quando a perda é exatamente 50% nenhuma chave pode ser extraída, devido ao fato de que Bob e Eva possuírem a mesma quantidade de informação $I_{AB} = I_{AE}$, o que implica $K \leq 0$. Essa não é uma falha de nosso protocolo, mas sim uma característica do ataque. Todos os protocolos que sofrem o ataque DF têm essa falha, que pode ser corrigida simplesmente com Alice adicionando propositalmente um pouco mais de perda. Para uma perda de 100%, ou seja, quando Eva rouba todo o sinal, algo interessante ocorre caso Eva realize todas as operações sobre o sinal roubado (100% dele) e Bob realize suas operações sobre o estado de vácuo (visto que Eva está com todo o sinal, o que sobra a Bob será o estado de vácuo). Para esse cenário o protocolo ainda continua funcionando perfeitamente para $|\alpha|$ pequeno.

Por mais estranho que pareça, as correlações criadas entre Alice e Bob devido às operações realizadas por Bob (lembrando que essas operações dependem de r, θ e das medidas de Alice) são maiores que as correlações entre Alice e Eva, $\beta I_{AB} > I_{AE}$ onde usamos $\beta = 0.8$. Uma possível explicação para isso, está no fato de que ao operar sobre o estado de vácuo Bob está mais "próximo" dos estados onde $|\alpha|$ é pequeno, necessitando assim de menos informação para reproduzir esses estados. Ele está livre das imperfeições produzidas pelo canal de emaranhamento finito. Eva, por outro lado, possui a mesma quantidade de informação que Bob (lembrando que ela realiza as mesma operações que Bob). No entanto, ela está sujeita as imperfeições produzidas pelo canal que, mesmo

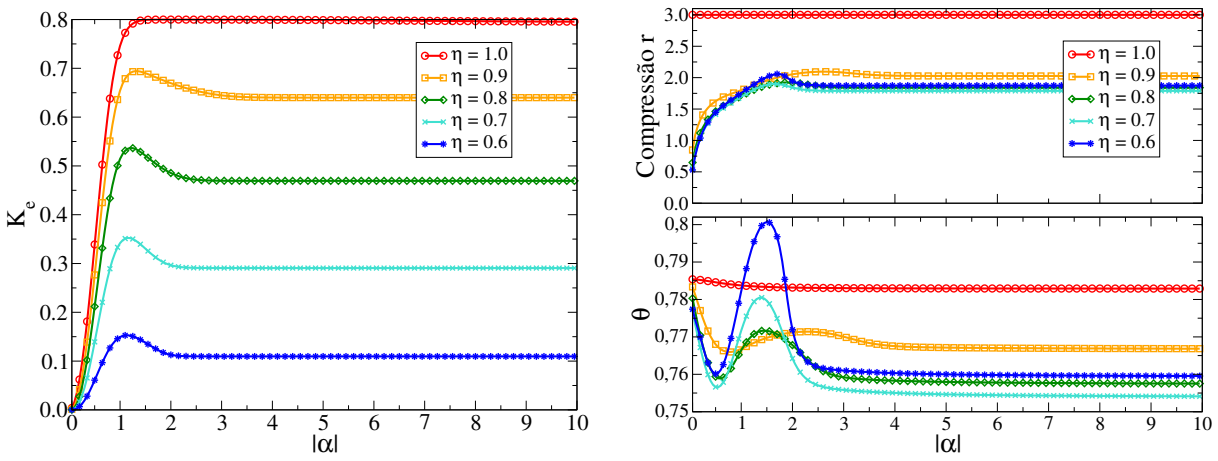


Figura 5.7: *(a) Aqui r e θ são ajustados de modo a obtermos as taxas de chave ótimas com $\beta = 0.8$, supondo a condição de coincidência do alfabeto real e η maiores que 0.6. (b) Parâmetros ótimos usados no calculo de K_e. No processo de maximização restringimos r de 0 a 3 com θ assumindo qualquer valor. Os valores ótimos de g_v e g_u são obtidos usando os valores de θ e r nas equações (5.17) e (5.18).*

para um fator de compressão da ordem de $r = 14$dB, ainda produz um teletransporte com eficiência menor que 0.7 para $|\alpha|$ pequeno (ver figura 5.2). Uma vez que $|\alpha|$ e a compressão do canal r são escolhido por Alice, mesmo utilizando 100% do sinal Eva não irá obter nenhuma parte da chave se Alice tomar $|\alpha|$ pequeno.

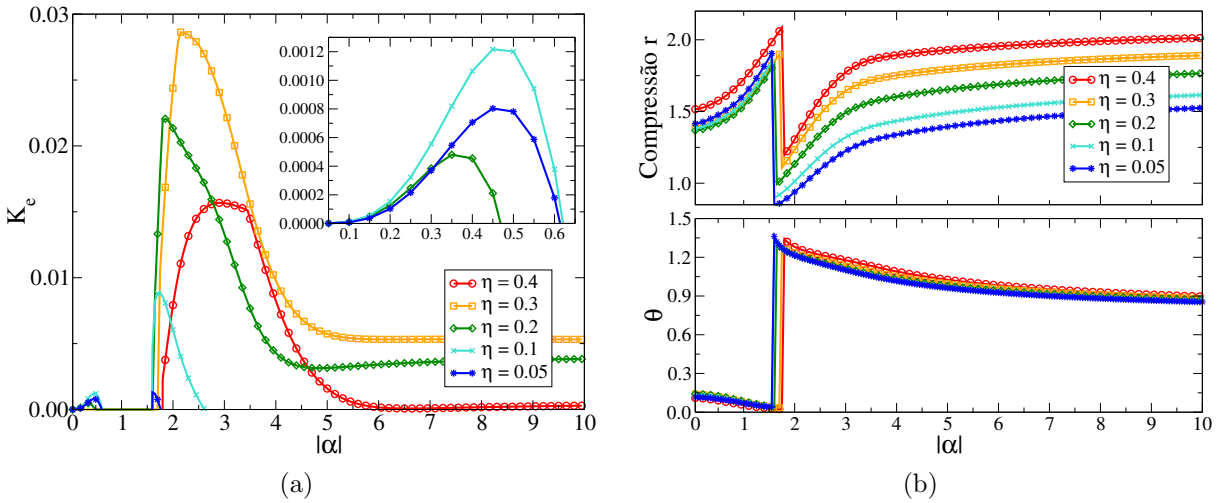


Figura 5.8: *(a)Aqui r e θ são ajustados de modo a obtermos as taxas de chave ótimas com $\beta = 0.8$, supondo a condição de coincidência do alfabeto real e η menores que 0.4. (b) Parâmetros ótimos usados no calculo de K_e. No processo de maximização nos restringimos r de 0 a 3 com θ assumindo qualquer valor. Os valores ótimos de g_v e g_u são obtidos usando os valores de θ e r nas equações (5.17) e (5.18).*

No entanto, Eva pode lançar mão de outro tipo de ataque. Roubando 100% do sinal e o descartando, fazendo uso apenas do estado de vácuo, assim como Bob. Nesse

cenário Bob e Eva possuem a mesma informação mútua com Alice, $I_{AB} = I_{AE}$, resultando em $K \leq 0$. Assim, para 100% de perda no sinal nosso protocolo deixaria de ser seguro. Isso sugere um possível ataque ao nosso protocolo, de modo que quando houver perdas elevadas no sinal Eva poderá escolher operar sobre o estado de vácuo, ao invés de operar em sua parte do estado interceptado. O que parece bastante razoável, visto que em ambientes de muita perda os estados do protocolo são mais próximos do estado de vácuo (veja figura 5.6). Devido a isso, uma melhor análise de segurança deve levar em conta que Eva trabalhará tanto com o sinal interceptado como com o estado de vácuo. Logo, nossa taxa de chave segura deve levar em conta esses dois ataques, de modo que podemos definir uma taxa de chave segura efetiva

$$K_e = \max\{0, \min\{\Delta I, \Delta I_0\}\}, \tag{5.56}$$

onde $\Delta I_0 = \beta I_{AB} - I^0_{AE}$ e I^0_{AE} é a informação mútua entre Alice e Eva, supondo que o estado de Eva é o estado de vácuo.

Usando g_u e g_v dados pelas expressões (5.17) e (5.18), onde ocorre a condição de correspondência, K_e se torna função apenas de r, θ e η. Fixando η, conseguimos otimizar K_e como uma função de r e θ uma vez escolhido o estado coerente $|\alpha\rangle$ (veja figuras 5.8 e 5.7). Trabalhando com $\beta = 0.8$, nós obtemos para uma perda de 90% (curva azul turquesa figura 5.8(a)) dois intervalos de α em que o protocolo é seguro. Para $|\alpha| \approx 0.5$ temos $K_e = 0.001$ com $r = 1.44$ (12.5dB) e para $|\alpha| \approx 1.75$ temos $K_e = 0.009$ com $r \approx 0.93$ (8.1dB). Quando consideramos uma perda de 95% (curva azul escuro, figura 5.8(a)) também conseguimos dois intervalos de $|\alpha|$ em que o protocolo é seguro. Para $|\alpha| \approx 0.5$, temos $K_e \approx 0.0008$ com $r \approx 1.47$ (12.8)dB e, para $|\alpha| \approx 1.6$, temos $K_e \approx 0.001$ com $r \approx 0.85$ (7.4)dB. As figuras (5.7(a)) e (5.8(a)) mostram K_e para diversas perdas no sinal. E os parâmetros ideais (ou ótimos) que levam a tais taxas de chave são dadas pelas figuras 5.7(b) e 5.8(b).

É interessante notar que sempre que temos perda ($\eta \neq 1$) o parâmetro de compressão (e por conseguinte o emaranhamento) ideal não é o maior valor possível. Para perdas menores que 50% (η de 1 a 0.6, figura 5.7(a)), quanto maior a perda menor a taxa de chave. Curiosamente, o comportamento para perdas maiores que 50% (η de 0.05 a 0.4, figura 5.8(a)) é diferente. Ao atravessar a fronteira de 50% de perda, quanto maior a perda melhor a taxa de chave. Mas essa tendência para a cerca de 70% de perda ($\eta = 0.3$). A partir desse marco a taxa de chave volta ao seu comportamento anterior diminuindo com a perda. Quando os valores das perda são exatos 50% ou 100%, nenhuma taxa de chave eficaz pode ser alcançada pois, como mencionamos anteriormente, Bob e Eva compartilham o mesmo nível de informação com Alice para esses valores de perdas. Observamos também que para a maioria dos casos, o parâmetro de compressão ideal não é maior do que $r = 2$ (17.4)dB.

Felizmente nosso protocolo funciona também com um baixo parâmetro de compressão, em especial se usarmos o estado da arte nos protocolos de reconciliação nos quais $\beta \approx 1$. Fixando r e usando g_u e g_v dados pelas equação (5.17) e (5.18), podemos maximizar K_e como uma função de θ. Mostramos com isso que para uma compressão baixa de $\approx$ 2dB ainda é possível obter uma chave segura (veja tabela 5.1). Na tabela 5.1 mostramos o máximo K_e atingível para diferentes valores de compressão e eficiência de reconciliação. Note que para $\beta = 0.8$ ou 0.9 nossa maximização numérica indica que não se pode obter uma chave segura quando as perdas se aproximam de 99%. No entanto, ao utilizar um parâmetro de eficiência $\beta \approx 1$ nosso protocolo funciona até mesmo para uma perda de 99% como mostra a tabela 5.1.

Tabela 5.1: *K_e para um parâmetro de eficiência de reconciliação fixa β, perda $1-\eta$, e uma compressão r com os parâmetros ótimos correspondentes. Assumimos um alfabeto real.*

β	loss	r(dB)	α	$\cos^2\theta$	g_u	g_v	K_e
0.8	95%	0.9(7.82)	1.65	0.058	0.957	0.632	2.9×10^{-3}
0.9	95%	0.7(6.08)	1.60	0.080	0.887	0.494	3.7×10^{-3}
1.0	99%	0.1(0.87)	1.50	0.114	0.186	0.068	3.0×10^{-6}
1.0	99%	0.2(1.74)	1.50	0.116	0.360	0.139	6.8×10^{-5}
1.0	99%	0.3(2.61)	1.50	0.108	0.516	0.206	4.2×10^{-4}
1.0	99%	0.4(3.47)	1.55	0.129	0.640	0.306	1.3×10^{-3}

Finalmente, é importante observar que, para as perdas inferiores a 50%, ou seja, quando mais de metade do sinal enviado a partir de Alice atinge Bob, a taxa de chave efetiva K_e é simplesmente K como dada pela equação (5.37). No entanto, quando a perda supera o nível de 50%, a equação (5.56) começa a ser relevante. Dependendo do valor de $|\alpha|$ e da perda, a chave será definida por ΔI ou ΔI_0. É por essa mudança de comportamento com perdas acima de 50% que as curvas para K_e (figura 5.8(a)) têm um comportamento brusco. E percebemos que para altas perdas, ΔI_0 é sempre utilizado, ou seja, para grandes perdas a informação mútua de Eva com Alice usando o vácuo é sempre maior que utilizando a parte do sinal roubada: $I^0_{AE} > I_{AE}$.

Em resumo, propusemos aqui um protocolo de DCQVC eficiente, com uma codificação binária para a chave (modulação discreta) baseado no PTVC de estado coerentes. Vale a pena destacar que o PTVC não é apenas um substituto para o envio direto de estados coerentes de Alice para Bob como nos protocolos usuais de DCQVC. Na verdade os recursos necessários para implementar o PTVC desempenham um papel direto na geração da chave secreta, desde a transmitância do DF de Alice, passando pela compressão do canal emaranhado e chegando até aos deslocamentos feitos por Bob. Um ajuste fino entre todos esses protocolos se faz necessário para gerar uma chave secreta.

Mostramos, também, que nosso protocolo de DCQVC baseado no PTVC é

seguro contra ataques individuais (ou ataques incoerentes) e, em particular, funciona com reconciliação direta e não faz uso de pós-seleção, mesmo para perdas muito elevadas no canal óptico que conecta Alice e Bob. Além disso, mostramos que é possível alcançar taxas de chave razoavelmente altas com um parâmetro de compressão baixo, $\approx$ 2dB, para um regime onde a perda no canal é próxima a 100%. Esse fato, juntamente com as altas taxas de repetição da tecnologia de variáveis contìnuas podem levar este protocolo de DCQVC a funcionar a longas distâncias de maneira eficiente. De fato, uma vez que um canal de dois modos emaranhados ligeiramente comprimido é estabelecido entre Alice e Bob, diretamente ou através de técnicas de entanglement swapping (troca de emaranhamento), eles podem gerar uma chave secreta usando nosso protocolo DCQVC.

Naturalmente, o sucesso desse protocolo frente ao ataque DF deixa algumas questões em aberto. Como, por exemplo, o quão robusto é esse protocolo ao se adicionar excesso de ruído na linha de transmissão? Podemos utilizar a reconciliação reversa e/ou a pós-seleção para aumentar a taxa de chave segura e diminuir ainda mais o parâmetro de compressão na geração da chave segura? Podemos estender a prova de segurança para ataques coletivos e coerentes? Podemos realizar a demostração da prova incondicional de segurança (unconditional security proof)? Como podemos ver, há muitas questões em aberto, as quais pretendemos responder em um futuro próximo.

No próximo capítulo iremos expor nossas considerações finais, relembrando os pontos relevantes dos capítulos anteriores e sugerindo possíveis assuntos a serem investigados futuramente.

Capítulo 6

Conclusão

A mudança de paradigma feita por Shannon em 1949 resultou em um grande avanço nas ciências da comunicação. Graças a essa mudança a informação pôde ser quantificada através de uma unidade básica de informação, o bit. Com essa quantificação da informação, tornou-se possível quantificar a compactação, transmissão e perda de informação. Outra mudança de paradigma, dessa vez tendo a mecânica quântica como protagonista, resultou em outro grande avanço na nossa habilidade de se comunicar. Os recursos oriundos da mecânica quântica, entre eles o emaranhamento, permitem a construção de protocolos que podem em princípio transmitir o dobro de informação comparados a protocolos clássicos, enviar informação criptografada com segurança garantida e até mesmo teleportar um sistema quântico.

Toda essa revolução na comunicação causada pela mecânica quântica teve início com protocolos baseados em variáveis discretas. Em seguida, outra mudança de paradigma dá início a teoria da comunicação quântica em variáveis contínuas, de modo que todos os protocolo descritos por variáveis discretas passam a ter o seu correspondente em variáveis contínuas, inclusive a transmissão "desencarnada" de informação, ou seja, o teletransporte quântico.

Nesta Tese aprofundamos o estudo do teletransporte quântico em variáveis contínuas. Para isso, iniciamos com uma revisão dos postulados da mecânica quântica no capítulo 2, a partir dos quais deduzimos as consequências mais relevantes ao tema desta Tese como, por exemplo, o teorema da não clonagem e a correlação quântica chamada emaranhamento. Este último é o recurso mais importante do protocolo de teletransporte quântico e com ele mostramos como realizar o teletransporte para variáveis discretas (qubit). Finalizamos o 2 realizando uma revisão de sistemas de variáveis contínuas, dando ênfase a sistemas Gaussianos.

No capítulo 3 estudamos o protocolo de teletransporte em variáveis contínuas. Iniciamos nosso estudo via o protocolo padrão (Braunstein and Kimble, 1998), só que de uma forma mais geral, de modo a investigar como alterações em sua implementação afetam a eficiência do protocolo. Ao procedermos dessa maneira, descobrimos a existência

de uma relação entre certos parâmetros usados na construção do protocolo que aparece ao maximizarmos sua eficiência. Ou seja, para obter a máxima fidelidade (eficiência) é necessário considerar de forma conjunta as escolhas que fazemos sobre a transmitância do divisor de feixes de Alice e os deslocamentos implementados por Bob. Demonstramos que, ao considerar o estado de entrada de Alice como um estado coerente qualquer, a melhor configuração para esses parâmetros é exatamente aquela do protocolo padrão (Braunstein and Kimble, 1998). No entanto, ao considerarmos uma possibilidade mais realística, ou seja, que $|\alpha\rangle$ está mais próximo do estado de vácuo, a configuração ótima é alterada.

De posse desse resultado, passamos a considerar os estados a serem teletransportados como sendo descritos também por distribuições centradas em diversos lugares do plano complexo. Passamos, pois, a considerar um cenário ainda mais realista, onde o experimentador pode escolher um estado dentro de uma distribuição de estados centrada em algum ponto do plano complexo. Com essa hipótese, mostramos que distribuições centradas nos eixos real ou imaginário alcançam os melhores resultados em termos da relação fidelidade por nível de emaranhamento do canal. Mostramos também que distribuições centradas no estado de vácuo possuem uma fidelidade alta mesmo com baixo parâmetro de compressão. Por fim vimos também que estados próximos aos eixos diagonais possuem fidelidade igual à dada pelo protocolo padrão.

No capítulo 4 criamos um protocolo de teletransporte multicanais, o qual pode ser visto como uma extensão natural do estudo apresentado no capítulo 3. Agora o estado a ser teletransportado é "divido" por Alice em n partes, com auxílio de divisores de feixes. Em seguida Alice combina cada uma dessas partes com sua parte do canal parcialmente emaranhado com Bob e as teleporta por meio de n canais independentes. Bob termina o protocolo recombinando estas n partes via n divisores de feixes e medindo as posições de $n-1$ estados. Especificamente, realizamos a análise do nosso protocolo considerando dois canais parcialmente emaranhados. Nessa configuração mostramos que nosso protocolo supera a eficiência do protocolo de multicanais sequencial de Yonezawa et al. (2007). Mostramos também que, utilizando dois canais parcialmente emaranhados, a eficiência do nosso protocolo é idêntica à do protocolo de teletransporte em variáveis contínuas (PTVC) original (Braunstein and Kimble, 1998) e superior ao protocolo híbrido de Andersen and Ralph (2013). Isso leva à seguinte pergunta: O que aconteceria ao introduzirmos mais canais ao protocolo? Este assunto será investigado futuramente.

No capítulo 5 realizamos uma aplicação direta do conhecimento adquirido no capítulo 3. Nesse capítulo mostramos um protocolo de criptografia que utiliza o teletransporte quântico de variáveis contínuas como sua espinha dorsal. Nosso protocolo funciona fazendo uso de dois alfabetos discretos compostos por 4 estados. Para $\alpha > 0$ chamamos de alfabeto real $\{|\alpha\rangle, |-\alpha\rangle\}$ e de alfabeto imaginário $\{|i\alpha\rangle, |-i\alpha\rangle\}$. Ao olharmos com mais atenção, esses estados são puramente reais ou imaginários, ou seja, são estados que estão distribuídos sobre os eixos onde obtivemos no capítulo 3 os melhores

resultados em eficiência.

Esse protocolo de criptografia é o primeiro que usa o teletransporte em variáveis contínuas diretamente na geração de chaves. Para analisar a robustez desse protocolo, estudamos o ataque de divisor de feixes. Este ataque consiste na espiã Eva roubar parte do sinal enviado a Bob e com essa parte do sinal tentar recuperar parte (ou toda) a chave. Mostramos que nosso protocolo é extremamente robusto para duas versões desse ataque. Na primeira versão, onde Eva rouba o sinal de Bob e tenta recuperar a chave a partir desse sinal, nosso protocolo é seguro até para 100% de perda do sinal. Na segunda versão, onde Eva rouba o sinal de Bob e descarta esse sinal realizando operações no estado de vácuo, mostramos que nosso protocolo é seguro até para 95% de perda no sinal. Ou seja, mesmo que Eva use as duas estratégias simultaneamente nosso protocolo é robusto ao ataque de divisor de feixes para perdas de até 95% do sinal. Além disso, este protocolo é o único que funciona com reconciliação direta e sem a necessidade de pós-seleção para perdas superiores a 50% até perdas próximas a 100%.

Em suma, nesta Tese estudamos o PTVC em detalhes. Mostramos que pequenas alterações no protocolo original que levem em conta a distribuição dos estados a serem teletransportados por Alice aumentam consideravelmente a eficiência do PTVC. Estendemos o PTVC para um cenário com muitos canais, criando um protocolo mais eficiente do que outros protocolos multicanais em variáveis contínuas. Mostramos também que nosso protocolo multicanais com dois canais em paralelo possui eficiência igual a eficiência do PTVC original. Desenvolvemos, também, com o conhecimento adquirido nos capítulos iniciais desta Tese, o primeiro protocolo de criptografia quântica robusto a ataques de divisores de feixes sem a necessidade de reconciliação reversa ou pós-seleção. Apesar de robusto a esse tipo de ataque, vale a pena lembrar que a criptografia é um jogo de gato e rato e o protocolo por nós proposto ainda necessita passar pelo crivo de outros ataques, os quais serão analisados em trabalhos futuros.

Apêndice A

Protocolo de criptografia RSA

O protocolo de criptografia RSA deve seu nome a seus três inventores, Ronald **R**ivest, Adi **S**hamir, e Leonard **A**dleman (Rivest et al., 1978). Ele é considerado um dos primeiros protocolos de criptografia a fazer uso de chaves assimétricas, ou seja, uma chave pública e outra privada. Porém, antes de detalhar esse protocolo, devemos descrever a notação usada na aritmética modular, explicar seu significado e definir a função totiente de Euler, ingredientes fundamentais para se entender o protocolo RSA.

A aritmética modular foi desenvolvida por Carl Friedrich Gauss em seu livro *Disquisitiones Arithmeticae*, publicado em 1801. Neste livro Gauss reunião resultados em teoria dos números obtidos por Pierre de Fermat, Leonhard Euler, Joseph-Louis Lagrande e Adrien-Marie Legendre, adicionando aos mesmos diversos resultados de sua autoria. No entanto, o desenvolvimento formal da aritmética modular foge do objetivo deste apêndice e por isso não o faremos aqui. O leitor interessado pode encontrar em Waterhouse et al. (1986) mais detalhes sobre esse assunto. Neste apêndice introduziremos a notação usada na aritmética modular por meio de um exemplo bem simples. Estamos nos referindo ao relógio de ponteiros.

Um relógio de ponteiros possui um conjunto finito de doze números inteiros (horas), de modo que, por exemplo, se agora são 7 horas, daqui a 8 horas serão 3 horas. Porém, a adição usual sugere que o tempo futuro deveria ser $7+8 = 15$ horas. No entanto, não exite o número 15 no relógio de ponteiros. O que fazemos ao utilizar o relógio de ponteiro é utilizar aritmética de módulo 12 $(\mathrm{mod}\, 12)$, onde $15 \equiv 3\,(\mathrm{mod}\, 12)$. Na soma o ponteiro é deslocado no sentindo horário e, quando alcança 12 horas, voltamos para zero. Na aritmética módulo 12 só temos os inteiros de 0 à 11 para expressar os valores das horas. Assim, de forma geral, a aritmética modular está relacionada com o resto da divisão pelo número que define a base da aritmética modular em que estamos trabalhando. Por exemplo, $2 = 14(\,\mathrm{mod}\, 12)$. Isso é verdade pois ao realizar a divisão de 14 por 12 temos um resto igual a 2. Vejamos outro exemplo, $2 = 14(\,\mathrm{mod}\, 12) = 38\,(\mathrm{mod}\, 12)$. Numa notação mais geral temos $a = b\,(\mathrm{mod}\, n)$, onde queremos dizer que o resto de a/n é igual ao resto de b/n. Note que quando $a, b < n$ temos $a\,(\mathrm{mod}\, n) = a$ e $b\ (\mathrm{mod}\, n) = b$. Muitas vezes

usa-se a notação $a = b \mod n$, evitando assim o uso do par de parênteses. Adotaremos esta convenção de agora em diante.

Uma vez esclarecido o significado da notação da aritmética modular, podemos definir a função totiente de Euler, também chamada de função tociente ou função $\varphi(x)$. Essa função é definida para um número natural x como sendo igual à quantidade de números menores ou iguais a x coprimos com respeito a ele (Rogers, 2010, pg.6). Matematicamente,

$$\varphi(x) = \#\left\{n \in \mathbb{N} | n \leq x \wedge \mathbb{mdc}(n, x) = 1\right\}. \tag{A.1}$$

De posse dessas definições podemos voltar ao protocolo. O protocolo funciona da seguinte maneira. Suponhamos que Alice deseje enviar a Bob uma mensagem através de um canal aberto (por canal aberto queremos dizer um canal onde outras pessoas podem ter acesso). Bob sabe que Alice deseja lhe enviar uma mensagem e Alice sabe que Bob é realmente quem diz ser. Bob então escolhe dois números primos grandes, p e q, e calcula $N = pq$. Bob também escolhe um número inteiro e tal que

$$\mathbb{mdc}(e, \varphi(N)) = 1, \tag{A.2}$$

onde $\phi(N)$ é a função totiente de Euler. A função totiente de Euler possui algumas propriedades interessantes. A primeira delas é que se p é um número primo então $\phi(p) = p-1$. A segunda é que se dois números são coprimos, p e q, então $\mathbb{mdc}(p, q) = 1$ e $\phi(pq) = \phi(p)\phi(q)$. Logo, Bob essencialmente está calculando $\mathbb{mdc}(e, (p-1)(q-1))$. Bob também calcula o número d, definido como

$$de = 1 \mod \varphi(N). \tag{A.3}$$

Ou seja, Bob calcula o inverso de e na aritmética modular definida por $\varphi(N)$. Após esse cálculo Bob envia para Alice N e e, os quais são chamados de *chave pública*, mantendo em segredo d, chamado de *chave privada*. Note que todos têm acesso a chave pública, incluindo o espião.

Alice, de posse de N e e, certifica-se de que sua mensagem x seja tal que $x < N$ e, usando a chave pública de Bob, codifica-a realizando o cálculo

$$y = C(x) = x^e \mod N. \tag{A.4}$$

Repare que Alice realiza o cálculo na aritmética de módulo N e que qualquer um, incluindo o espião, pode realizar essa operação já que N e e são públicos. Ou seja, qualquer um tem acesso a chave de encriptação. Após encriptar sua mensagem, Alice envia y a Bob que, para acessar o conteúdo da mensagem, deve realizar uma operação que inverta a conta

feita por Alice, obtendo

$$D(y) = x. \tag{A.5}$$

Para isso Bob escolhe $D(y)$ da seguinte forma,

$$D(y) = x^{ed} \mod N. \tag{A.6}$$

Note que só Bob tem acesso ao número d, a chave privada, e que $y = x^e \mod N$. Conforme provamos a seguir, usando o d correto a eq. (A.6) dá $x^{ed} \mod N = x$ e Bob recupera a mensagem.

Uma vez que $ed = 1 \mod \phi(N)$ e a mensagem está encriptada na aritmética de módulo N, deve existir um inteiro k tal que $ed = 1 + k\phi(N) \mod N$. Dessa forma como Bob sabe que $y = e^x$

$$\begin{aligned} D(y) &= x^{1+k\phi(N)} \mod N, \\ &= xx^{k\phi(N)} \mod N, \\ &= x(x^{\phi(N)})^k \mod N. \end{aligned} \tag{A.7}$$

De acordo com o teorema de Euler-Fermat (Martinez et al., 2010, pg.50) temos que para qualquer inteiro coprimo positivo N e a, $a^{\phi(N)} = 1 \mod N$. Logo, como x e N são coprimos temos

$$D(y) = x(1^k) \mod N = x \mod N = x. \tag{A.8}$$

O passo final se justifica pois $x < N$. Após aplicar a operação $D(y)$ Bob recupera a mensagem original de Alice. Note que apenas Bob possui a informação sobre d. Dessa maneira apenas ele pode recuperar a mensagem.

Ao executar o protocolo Bob divulga abertamente informações sobre a chave pública, e e N. Uma pergunta pertinente é: De posse dessas informações a espiã Eva não poderia recuperar a mensagem x de Alice? Ao analisarmos a chave pública, temos que e é membro do grupo de inteiros da aritmética de módulo N, possuindo um único inverso dado por d (Rogers, 2010, pg.7). Devido ao fato de Bob manter d em segredo, Eva não possui conhecimento de como calcular $D(y)$. No entanto, Eva pode calcular d, encontrando o valor de $\phi(N)$. Porém, calcular a função totiente de Euler não é uma tarefa simples, uma vez que N tem centenas ou milhares de dígitos. Dada as propriedades da função $\phi(N)$, a maneira mais eficiente de calculá-la é fatorar N em fatores primos, uma tarefa considerada até hoje computacional complexa.

Um algoritmo de fatoração eficiente não existe e a busca por tal algoritmo é o santo graal da matemática moderna (Rogers, 2010, pg.7). Em termos da teoria de

complexidade computacional, esse problema faz parte da classe de problemas conhecidos como Tempo Polinomial Não Determinístico - Completo (Nondeterministic Polynomial Time- Complete), ou NP-completo. Os problemas NP-completos têm algumas propriedades importantes. Uma delas é que deve existir um algoritmo eficiente (ou seja, que opere em um tempo polinomial) que verifique a solução do problema. No caso do protocolo RSA é óbvio que ao ter acesso a p Eva pode verificar se esse é um fator primo de N por uma simples divisão. A segunda propriedade dos problemas NP-completos é que nenhuma solução eficiente para algum destes problemas foi encontrada. Até hoje, o algoritmo de fatoração mais eficiente é o algoritmo GNFS (General Number Field Sieve), que opera em um tempo assimptótico sub-exponencial

$$O\left(\exp\left(\left(\frac{64}{9}n\right)^{\frac{1}{3}}(\log(n))^{\frac{2}{3}}\right)\right), \tag{A.9}$$

onde $n = \log N$. Para se ter uma ideia da dificuldade do problema, a fatoração de um número de 250 dígitos demoraria 10 milhões de anos á taxa de cálculo de 200-MHz (milhões de instruções por segundo) (Benenti et al., 2004, pg.194).

Devido ao tempo de execução extremamente longo para N grande, a obtenção dos fatores p e q se torna inviável. Desse modo, Bob garante a segurança do protocolo pela inexistência de um protocolo eficiente em fatorar números primos. Essa segunda propriedade é interessante pois não existe prova de que Eva não possa obter os fatores primos de N em um tempo polinomial P, o que significaria que $NP = P$. Assim, a segurança do protocolo é garantida supondo que $NP \neq P$. Embora não haja nenhuma prova desse fato, cientistas da computação e matemáticos (como os autores do protocolo) acreditam que $NP \neq P$ e que nenhum algoritmo possa fatorar números primos em tempo polinomial.

Para uma melhor visualização do funcionamento do protocolo RSA, vamos considerar um exemplo numérico de seu funcionamento. Bob primeiro escolhe $N = pq = 5 \times 11$ e em seguida o inteiro $e = 3$, de modo que satisfaça

$$\mathbb{mdc}(e, (p-1)(q-1)) = \mathbb{mdc}(3, (5-1)(11-1)) = 1, \tag{A.10}$$

Bob prossegue calculando o inverso de e na aritmética de módulo $\varphi(N) = (p-1)(q-1) = (5-1)(11-1) = 40$,

$$de = 1 \mod \varphi(N) \rightarrow d = 27. \tag{A.11}$$

Bob envia a Alice de forma pública N e e. Alice de posse desses números realiza a codi-

ficação da sua mensagem. Vamos supor $x = 9$. Dessa forma,

$$y = C(9) = 9^3 \mod 55 = 729 \mod 55 = 14. \tag{A.12}$$

Alice envia a Bob a mensagem codificada $y = 14$. Bob decodifica a mensagem aplicando a operação inversa. Lembrando que $d = 27$, a eq. (A.6) vale

$$\begin{aligned} D(y) &= 14^{27} \mod 55, \\ &= 8.819.763.977.946.281.130.444.984.418.304 \mod 55 = 9. \end{aligned} \tag{A.13}$$

Veja que Bob recupera exatamente a mensagem enviada por Alice, $x = D(y) = 9$. Note que sem o valor correto de d, Eva não sabe qual expoente usar para realizar a operação inversa. Por exemplo, se ela usar $d = 26$ temos $D(y) = 36$ e se usar $d = 28$ temos $D(y) = 16$. Ou seja, errando de apenas uma unidade o valor correto de d, a chave privada, Eva obtém mensagens totalmente diferentes.

Apêndice B

Desigualdade de Schwarz

A desigualdade de Schwarz afirma que para quaisquer dois vetores vale a relação

$$|\langle\varphi|\psi\rangle|^2 \leq \langle\varphi|\varphi\rangle\langle\psi|\psi\rangle. \tag{B.1}$$

Para demonstrá-la vamos usar a propriedade do produto escalar $\langle\chi|\chi\rangle \geq 0$. Sendo $|\chi\rangle = |\varphi\rangle + z|\psi\rangle$, onde z é um número complexo, temos

$$\langle\varphi + z\psi|\varphi + z\psi\rangle \geq 0, \tag{B.2}$$

$$\langle\varphi|\varphi\rangle + z\langle\varphi|\psi\rangle + z^*\langle\psi|\varphi\rangle + |z|^2\langle\psi|\psi\rangle \geq 0, \tag{B.3}$$

onde usamos a linearidade (antiliniaridade) dos kets (bras). A igualdade é valida se os vetores são nulos. Caso contrário tomamos $z = -\langle\psi|\varphi\rangle/\langle\psi|\psi\rangle$ e usando $\langle\psi|\varphi\rangle^* = \langle\varphi|\psi\rangle$ obtemos

$$\langle\varphi|\varphi\rangle - 2\frac{|\langle\varphi|\psi\rangle|^2}{\langle\psi|\psi\rangle} + \frac{|\langle\varphi|\psi\rangle|^2}{\langle\psi|\psi\rangle} > 0. \tag{B.4}$$

Isso implica a desigualdade procurada,

$$|\langle\varphi|\psi\rangle|^2 \leq \langle\varphi|\varphi\rangle\langle\psi|\psi\rangle. \tag{B.5}$$

Apêndice C

Teoremas

C.1 Teorema I

Queremos provar que se o operador $\hat{A}$ é Hermitiano então todos os seus autovalores são reais. Para realizar a demonstração vamos usar a definição de operador Hermitiano. Se $\hat{A}$ é Hermitiano temos $\langle\varphi|\hat{A}\varphi\rangle = \langle\varphi|\hat{A}|\varphi\rangle^*$. Como $\hat{A}|\varphi\rangle = a|\varphi\rangle$ podemos substituir isso na última equação de modo que

$$\begin{aligned} \langle\varphi|a|\varphi\rangle &= \langle\varphi|a|\varphi\rangle^* \\ a\langle\varphi|\varphi\rangle &= a^*\langle\varphi|\varphi\rangle \end{aligned}$$

Isto implica $a = a^*$ uma vez que apenas vetores não nulos são considerados como soluções não triviais da equação de autovetor.

C.2 Teorema II

Queremos provar que autovetores que correspondem a autovalores distintos para um operador Hermitiano devem ser ortogonais. Para demostrar faremos uso da definição de operador Hermitiano. Se $\hat{A}$ é um operador Hermitiano, então $\langle\varphi_1|\hat{A}|\varphi_2\rangle = \langle\varphi_2|\hat{A}|\varphi_1\rangle^*$. Logo,

$$0 = \langle\varphi_1|\hat{A}|\varphi_2\rangle - \langle\varphi_2|\hat{A}|\varphi_1\rangle^*.$$

Como $\hat{A}|\varphi_1\rangle = a_1|\varphi_1\rangle$ e $\hat{A}|\varphi_2\rangle = a_2|\varphi_2\rangle$ temos

$$\begin{aligned} 0 &= a_1\langle\varphi_2|\varphi_1\rangle - a_2\langle\varphi_1|\varphi_2\rangle^* \\ 0 &= (a_1 - a_2)\,\langle\varphi_2|\varphi_1\rangle. \end{aligned}$$

Portanto $\langle\varphi_2|\varphi_1\rangle = 0$ se $a_1 \neq a_2$, i.e., temos vetores ortogonais.

Apêndice D

Relação de comutação entre posição e momento

Para realizar a demonstração vamos calcular a média de $[\hat{x}, \hat{p}]$. Assim,

$$\langle x| \left[\hat{x}, \hat{p}\right] |\phi\rangle = \langle x|\hat{x}\hat{p}|\phi\rangle - \langle x|\hat{p}\hat{x}|\phi\rangle.$$

Atuando os operadores temos

$$\langle x| \left[\hat{x}, \hat{p}\right] |\phi\rangle = x\left(-\imath\hbar\frac{d}{dx}\right)\langle x|\phi\rangle - \left(-\imath\hbar\frac{d}{dx}\right)x\langle x|\phi\rangle,$$

onde usamos que $\langle x|\hat{x}|\phi\rangle \equiv x\langle x|\phi\rangle$ e $\langle x|\hat{p}|\phi\rangle \equiv -\imath\hbar\frac{d}{dx}\langle x|\phi\rangle$. Usando que $\langle x|\phi\rangle = \phi(x)$, temos

$$\langle x| \left[\hat{x}, \hat{p}\right] |\phi\rangle = x\left(-\imath\hbar\frac{d}{dx}\right)\phi(x) - \left(-\imath\hbar\frac{d}{dx}\right)x\phi(x),$$

$$\langle x| \left[\hat{x}, \hat{p}\right] |\phi\rangle = -x\imath\hbar\frac{d\phi(x)}{dx} + \imath\hbar\phi(x) + \imath\hbar x\frac{d\phi(x)}{dx},$$

$$\langle x| \left[\hat{x}, \hat{p}\right] |\phi\rangle = \imath\hbar\phi(x),$$

$$\langle x| \left[\hat{x}, \hat{p}\right] |\phi\rangle = \langle x|\imath\hbar|\phi\rangle.$$

Portanto

$$\left[\hat{x}, \hat{p}\right] = i\hbar. \tag{D.1}$$

Apêndice E

Estado de vácuo comprimido de dois modos

Neste apêndice iremos encontrar a representação do estado de vácuo comprimido de dois modos na base da posição. Esse estado pode ser obtido aplicando-se o operador de compressão (Braunstein and van Loock, 2005, p.524) ao estado de vácuo,

$$|\psi\rangle = \exp\left\{-r\left(\hat{a}_1\hat{a}_2 e^{-i\varphi} - \hat{a}_1^\dagger\hat{a}_2^\dagger e^{i\varphi}\right)\right\}|00\rangle\ . \tag{E.1}$$

Usando a relação (Schumaker and Caves, 1985)

$$\exp\left\{r\left(\hat{a}_1\hat{a}_2 e^{-i\varphi} - \hat{a}_1^\dagger\hat{a}_2^\dagger e^{i\varphi}\right)\right\} = e^{e^{i\varphi}\tanh(r)\hat{a}_1^\dagger\hat{a}_2^\dagger} e^{-\ln(\cosh(r))\left(1+\hat{a}_1^\dagger\hat{a}_1+\hat{a}_2^\dagger\hat{a}_2\right)} e^{-e^{-i\varphi}\tanh(r)\hat{a}_1\hat{a}_2}, \tag{E.2}$$

temos

$$|\psi\rangle\ = e^{e^{i\varphi}\tanh(r)\hat{a}_1^\dagger\hat{a}_2^\dagger} e^{-\ln(\cosh(r))\left(1+\hat{a}_1^\dagger\hat{a}_1+\hat{a}_2^\dagger\hat{a}_2\right)} e^{-e^{-i\varphi}\tanh(r)\hat{a}_1\hat{a}_2}\,|00\rangle\ . \tag{E.3}$$

A aplicação do operador de aniquilação no estado de vácuo resulta em um autovalor nulo, de modo que

$$|\psi\rangle = \frac{1}{\cosh(r)}\exp\left\{e^{i\varphi}\tanh(r)\,\hat{a}_1^\dagger\hat{a}_2^\dagger\right\}|00\rangle\ . \tag{E.4}$$

Escrevendo a exponencial na forma de somatória

$$|\psi\rangle = \frac{1}{\cosh(r)}\sum_n \frac{\left(e^{i\varphi}\tanh(r)\,\hat{a}_1^\dagger\hat{a}_2^\dagger\right)^n}{n!}|00\rangle \tag{E.5}$$

e aplicando o operador de criação temos

$$|\psi\rangle = \frac{1}{\cosh(r)}\sum_n \left(e^{i\varphi}\tanh(r)\right)^n|nn\rangle\ . \tag{E.6}$$

Multiplicando o lado direito por $1 = \int dx_j \left|x_j\right\rangle\left\langle x_j\right|$, onde $j = 1, 2$, temos

$$\left|\psi\right\rangle = \frac{1}{\cosh\left(r\right)} \sum_n \left(e^{i\varphi} \tanh\left(r\right)\right)^n \int dx_1 dx_2 \left|x_1\right\rangle \left|x_2\right\rangle \left\langle x_1\right| n\rangle \left\langle x_2\right| n\rangle. \tag{E.7}$$

Precisamos agora calcular $\langle x_i|n\rangle$. Como $\hat{a}\left|0\right\rangle = 0$, onde $\hat{a} = \hat{x} + i\hat{p}$, temos $\left(\hat{x} + i\hat{p}\right)\left|0\right\rangle = 0$. Logo, aplicando $\left\langle \hat{x}'\right|$ em ambos os lados obtemos

$$\left\langle \hat{x}'\right|\left(\hat{x} + i\hat{p}\right)\left|0\right\rangle = \left\langle \hat{x}'\right|\hat{x}\left|0\right\rangle + i\left\langle \hat{x}'\right|\hat{p}\left|0\right\rangle = \left(x' + \frac{1}{2}\frac{d}{dx'}\right)\left\langle x'\right|0\rangle = 0, \tag{E.8}$$

onde usamos a convenção adotada na teoria de informação quântica de $\hbar = 1/2$. Resolvendo a eq. diferencial acima temos

$$\left\langle x'\right|0\rangle = \left(\frac{2}{\pi}\right)^{1/4} \exp\left\{-x'^2\right\}, \tag{E.9}$$

onde a constante foi fixada impondo a normalização $\int \left|\left\langle x'\right|0\rangle\right|^2 dx' = 1$. Lembrando que os polinômios de Hermite são

$$H_n\left(x\right) = \left(-1\right)^n e^{x^2} \frac{d^n}{dx^n} e^{-x^2}, \tag{E.10}$$

temos

$$\left\langle x'\right|0\rangle = \left(\frac{2}{\pi}\right)^{1/4} H_0\left(\sqrt{2}x'\right) \exp\left\{-x'^2\right\}. \tag{E.11}$$

Em geral

$$\left\langle x'\right|n\rangle = \left(\frac{2}{\pi}\right)^{1/4} \frac{1}{2^{\frac{n}{2}}\sqrt{n!}} H_n\left(\sqrt{2}x'\right) \exp\left\{-x'^2\right\}, \tag{E.12}$$

onde a expressão acima pode ser demostrada por indução. Finalmente podemos reescrever a equação (E.7) como

$$\begin{aligned} \left|\psi\right\rangle &= \left(\frac{2}{\pi\cosh^2\left(r\right)}\right)^{\frac{1}{2}} \int dx_1 dx_2 e^{-\left(x_1^2 + x_2^2\right)} \\ &\quad \times \sum_n \left(\frac{e^{i\varphi}\tanh\left(r\right)}{2}\right)^n \frac{H_n\left(\sqrt{2}x_1\right) H_n\left(\sqrt{2}x_2\right)}{n!} \left|x_1, x_2\right\rangle. \end{aligned} \tag{E.13}$$

Usando a formula de Melher (Veja apêndice F)

$$\sum_n \left(\frac{z}{2}\right)^n \frac{H_n\left(x\right) H_n\left(y\right)}{n!} = \frac{1}{\sqrt{1 - z^2}} \exp\left\{\frac{z\left(2xy - zx^2 - zy^2\right)}{\left(1 - z^2\right)}\right\}, \tag{E.14}$$

onde $x = \sqrt{2}x_1$, $y = \sqrt{2}x_2$ e $z = e^{i\varphi}\tanh(r)$ temos

$$|\psi\rangle = \left(\frac{2}{\left(1 - e^{2i\varphi}\tanh^2(r)\right)\pi\cosh^2(r)}\right)^{\frac{1}{2}} \int dx_1 dx_2 \exp\left\{ -\left(x_1^2 + x_2^2\right) + e^{i\varphi}\tanh(r)\,\frac{\left(4x_1x_2 - 2e^{i\varphi}\tanh(r)\,x_1^2 - 2e^{i\varphi}\tanh(r)\,x_2^2\right)}{\left(1 - e^{2i\varphi}\tanh^2(r)\right)}\right\}|x_1, x_2\rangle\,. \quad \text{(E.15)}$$

Usando que $\tanh(r) = \sinh(r)/\cosh(r)$ e que

$$\sinh(r) = \frac{e^r - e^{-r}}{2}, \quad \cosh(r) = \frac{e^r + e^{-r}}{2} \quad \text{(E.16)}$$

obtemos

$$|\psi\rangle = \left(\frac{2}{\pi\left(\cosh^2(r) - e^{2i\varphi}\sinh^2(r)\right)}\right)^{\frac{1}{2}} \int dx_1 dx_2 \exp\left\{\frac{1}{\left(\cosh^2(r) - e^{2i\varphi}\sinh^2(r)\right)} \times \left[-\frac{e^{2r}}{4}\left[\left(x_1 - x_2e^{i\varphi}\right)^2 + \left(x_1e^{i\varphi} - x_2\right)^2\right] - \frac{e^{-2r}}{4}\left[\left(x_1 + x_2e^{i\varphi}\right)^2 + \left(x_1e^{i\varphi} + x_2\right)^2\right] - \frac{1}{2}\left(x_1^2 + x_2^2 - \left(x_1^2 + x_2^2\right)e^{2i\varphi}\right)\right]\right\}|x_1, x_2\rangle\,. \quad \text{(E.17)}$$

Quando $\varphi = 0$ obtemos

$$|\psi\rangle = \left(\frac{2}{\pi}\right)^{\frac{1}{2}} \int dx_1 dx_2 \exp\left\{\left[-\frac{e^{2r}}{2}\left[(x_1 - x_2)^2\right] - \frac{e^{-2r}}{2}\left[(x_1 + x_2)^2\right]\right]\right\}|x_1, x_2\rangle\,. \quad \text{(E.18)}$$

Esse estado pode ser encontrado em Braunstein and van Loock (2005) e em Leonhardt (1997), embora a dedução da eq.(E.18) não se encontre em nenhuma delas. De posse da equação do estado podemos agora calcular o valor médio $\langle(\hat{x}_1 - \hat{x}_2)^2\rangle$. Assim

$$\langle(\hat{x}_1 - \hat{x}_2)^2\rangle = \langle\hat{x}_1^2 - \hat{x}_1\hat{x}_2 - \hat{x}_2\hat{x}_1 + \hat{x}_2^2\rangle = \langle\hat{x}_1^2\rangle - 2\langle\hat{x}_1\hat{x}_2\rangle + \langle\hat{x}_2^2\rangle, \quad \text{(E.19)}$$

onde

$$\langle f(\hat{x}_1, \hat{x}_2)\rangle = \int dx_1 dx_2 f(x_1, x_2)|\psi(x_1, x_2)|^2. \quad \text{(E.20)}$$

Realizando as integrais temos

$$\langle\hat{x}_1^2\rangle = \frac{1}{4}\cosh(2r)\,, \quad \langle\hat{x}_1\hat{x}_2\rangle = \frac{1}{4}\cos(\varphi)\sinh(2r) \quad \text{e} \quad \langle\hat{x}_2^2\rangle = \frac{1}{4}\cosh(2r)\,. \quad \text{(E.21)}$$

Logo

$$\langle(\hat{x}_1 - \hat{x}_2)^2\rangle = \frac{1}{2}\left(\cosh(2r) - \cos(\varphi)\sinh(2r)\right) \quad \text{(E.22)}$$

e quando $\varphi = 0$

$$\langle (\hat{x}_1 - \hat{x}_2)^2 \rangle = \frac{e^{-2r}}{2}. \tag{E.23}$$

Analogamente temos

$$\langle (\hat{x}_1 + \hat{x}_2)^2 \rangle = \frac{1}{2} \left(\cosh(2r) + \cos(\varphi) \sinh(2r) \right) \tag{E.24}$$

e quando $\varphi = 0$ temos

$$\langle (\hat{x}_1 + \hat{x}_2)^2 \rangle = \frac{e^{2r}}{2}. \tag{E.25}$$

Agora lembrando que

$$\langle g(\hat{p}_1, \hat{p}_2) \rangle = \int dx_1 dx_2 \psi^*(x_1, x_2) g\left(\frac{\hbar}{i} \frac{\partial}{\partial x_1}, \frac{\hbar}{i} \frac{\partial}{\partial x_2} \right) \psi(x_1, x_2) \tag{E.26}$$

temos

$$\langle \hat{p}_1^2 \rangle = \frac{1}{4} \cosh(2r), \quad \langle \hat{p}_1 \hat{p}_2 \rangle = -\frac{1}{4} \cos(\varphi) \sinh(2r) \quad \text{e} \quad \langle \hat{p}_2^2 \rangle = \frac{1}{4} \cosh(2r). \tag{E.27}$$

Portanto,

$$\langle (\hat{p}_1 + \hat{p}_2)^2 \rangle = \frac{1}{2} \left(\cosh(2r) - \cos(\varphi) \sinh(2r) \right). \tag{E.28}$$

E quando $\varphi = 0$

$$\langle (\hat{p}_1 + \hat{p}_2)^2 \rangle = \frac{e^{-2r}}{2}. \tag{E.29}$$

Para a diferença temos

$$\langle (\hat{p}_1 - \hat{p}_2)^2 \rangle = \langle \hat{p}_1^2 \rangle - 2\langle \hat{p}_1 \hat{p}_2 \rangle + \langle \hat{p}_2^2 \rangle, \tag{E.30}$$

$$\langle (\hat{p}_1 - \hat{p}_2)^2 \rangle = \frac{1}{4} \cosh(2r) + \frac{2}{4} \cos(\varphi) \sinh(2r) + \frac{1}{4} \cosh(2r) = \frac{e^{2r}}{2}. \tag{E.31}$$

Ao observamos as quadraturas individuais $\hat{x}_k$ e $\hat{p}_k$, onde $k = \{1, 2\}$, vemos que essas se tornam muito ruidosas ao se aumentar a compressão r. No entanto, esse ruído se torna menor na posição relativa $(\hat{x}_1 - \hat{x}_2)$ e no momento total $(\hat{p}_1 + \hat{p}_2)$, indo a zero quando $r \to \infty$ (Braunstein and van Loock, 2005, pg. 525). Para ilustrar o significado desse ruído indo a zero e as consequências contraintuitivas de se interpretar o emaranhamento à luz da física clássica, vamos considerar que as quadraturas pertençam a partículas clássicas. As quadraturas com índice 1 pertencem à partícula 1 e as quadraturas com índice 2 pertencem à partícula 2. Logo, ao calcularmos a posição relativa e o momento total dessas partículas para uma compressão infinita $r = \infty$, temos como resultado $\hat{x}_1 - \hat{x}_2 = 0$ e $\hat{p}_1 + \hat{p}_2 = 0$. Classicamente isso significaria que as partículas ocupam a mesma posição com momentos de sinais opostos, de modo que a modificação na velocidade de uma partícula seria compensada pela mudança contrária na outra, mantendo a posição relativa igual

a zero. Porém, vimos no capítulo 3 que essas "partículas" ocupam posições espaciais diferentes, não sendo portanto a interpretação clássica acima correta. A posição relativa e o momento total das partículas calculadas em $r = \infty$ mostram que esse sistema não pode mais ser considerado separadamente devendo sim ser tratado como uma única entidade. Ou seja, o estado que descreve essas partículas é o que chamamos em mecânica quântica de um estado maximamente emaranhado. O estado de vácuo comprimido de dois modos é o representante mais famoso da óptica quântica para emaranhamento bipartido em variáveis contínuas (Braunstein and van Loock, 2005, pg. 525).

Apêndice F

Fórmula de Mehler

Neste apêndice iremos deduzir a fórmula de Mehler. Para essa demonstração iremos usar a fórmula de Rodrigues, ou representação de Rodrigues, para os polinômios de Hermite (Arfken and Weber, 2005, p.819):

$$H_n(x) = (-1)^n e^{x^2} \left(\frac{d}{dx}\right)^n e^{-x^2}. \tag{F.1}$$

Como

$$e^{-x^2} = \frac{1}{\sqrt{\pi}} \int_{-\infty}^{+\infty} e^{-\epsilon^2 + 2ix\epsilon} d\epsilon \tag{F.2}$$

a fórmula de Rodrigues fica

$$H_n(x) = (-1)^n e^{x^2} \left(\frac{d}{dx}\right)^n \frac{1}{\sqrt{\pi}} \int_{-\infty}^{+\infty} e^{-\epsilon^2 + 2ix\epsilon} d\epsilon = \frac{1}{\sqrt{\pi}} \int_{-\infty}^{+\infty} (-2i\epsilon)^n e^{-(\epsilon - ix)^2} d\epsilon. \tag{F.3}$$

Agora possuimos uma representação na forma integral para os polinômios de Hermite. Assim,

$$\begin{aligned}
\sum_n \left(\frac{z}{2}\right)^n \frac{H_n(x_1) H_n(x_2)}{n!} &= \sum_n \left(\frac{z}{2}\right)^n \frac{1}{n!} \frac{1}{\pi} \int_{-\infty}^{+\infty} \int_{-\infty}^{+\infty} d\epsilon d\eta \, (-2i\epsilon)^n e^{-(\epsilon - ix_1)^2} (-2i\eta)^n e^{-(\eta - ix_2)^2} \\
&= \frac{1}{\pi} \int_{-\infty}^{+\infty} \int_{-\infty}^{+\infty} d\epsilon d\eta \sum_n \frac{1}{n!} (-z2\epsilon\eta)^n e^{-(\epsilon - ix_1)^2} e^{-(\eta - ix_2)^2} \\
&= \frac{1}{\pi} \int_{-\infty}^{+\infty} \int_{-\infty}^{+\infty} d\epsilon d\eta e^{-z2\epsilon\eta} e^{-(\epsilon - ix_1)^2} e^{-(\eta - ix_2)^2}.
\end{aligned} \tag{F.4}$$

Resolvendo as integrais obtemos então a fórmula de Mehler,

$$\sum_n \left(\frac{z}{2}\right)^n \frac{H_n(x_1) H_n(x_2)}{n!} = \frac{\exp\left\{\frac{\left(2x_1x_2 - \left(x_1^2 + x_2^2\right)z\right)z}{1-z^2}\right\}}{\sqrt{1-z^2}}. \tag{F.5}$$

Referências Bibliográficas

Adesso, G. (2006), Entanglement of Gaussian States, Doutorado, Facoltà di Scienze Matematiche Fisiche e Naturali.

Andersen, U. L. and Ralph, T. C. (2013), 'High-fidelity teleportation of continuous-variable quantum states using delocalized single photons', *Phys. Rev. Lett.* **111**, 050504.

Arfken, G. and Weber, H. (2005), *Mathematical Methods for Physicists*, Mathematical Methods for Physicists, Elsevier.

Atkinson, Q. D. (2011), 'Phonemic diversity supports a serial founder effect model of language expansion from africa', *Science* **332**(6027), 346–349.

Ballentine, L. (1998), *Quantum Mechanics: A Modern Development*, World Scientific.

Ban, M. (1999), 'Quantum dense coding via a two-mode squeezed-vacuum state', *Journal of Optics B: Quantum and Semiclassical Optics* **1**(6), L9.

Barnum, H. N. I. (1998), Quantum Information Theory, Doutorado, University of New Mexico, Albuquerque.

Benenti, G., Casati, G. and Strini, G. (2004), *Principles of Quantum Computation and Information: Basic concepts*, Principles of Quantum Computation and Information, World Scientific.

Bennett, C. H. and Brassard, G. (1984), Quantum cryptography: Public key distribution and coin tossing, *in* 'Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing', p. 175.

Bennett, C. H., Brassard, G., Crépeau, C., Jozsa, R., Peres, A. and Wootters, W. K. (1993), 'Teleporting an unknown quantum state via dual classical and einstein-podolsky-rosen channels', *Phys. Rev. Lett.* **70**, 1895–1899.

Bennett, C. H. and Wiesner, S. J. (1992), 'Communication via one- and two-particle operators on einstein-podolsky-rosen states', *Phys. Rev. Lett.* **69**, 2881–2884.

Boschi, D., Branca, S., De Martini, F., Hardy, L. and Popescu, S. (1998), 'Experimental realization of teleporting an unknown pure quantum state via dual classical and einstein-podolsky-rosen channels', *Phys. Rev. Lett.* **80**, 1121–1125.

Bouwmeester, D., Pan, J.-W., Mattle, K., Eibl, M., Weinfurter, H. and Zeilinger, A. (1997), 'Experimental quantum teleportation', *Nature* **390**, 575.

Bowen, W. P., Treps, N., Buchler, B. C., Schnabel, R., Ralph, T. C., Bachor, H.-A., Symul, T. and Lam, P. K. (2003), 'Experimental investigation of continuous-variable quantum teleportation', *Phys. Rev. A* **67**, 032302.

Bowen, W., Treps, N., Buchler, B., Schnabel, R., Ralph, T., Symul, T. and Lam, P. K. (2003), 'Unity gain and nonunity gain quantum teleportation', *Selected Topics in Quantum Electronics, IEEE Journal of* **9**(6), 1519–1532.

Braunstein, S. L., Fuchs, C. A. and Kimble, H. J. (2000), 'Criteria for continuous-variable quantum teleportation', *Journal of Modern Optics* **47**(2-3), 267–278.

Braunstein, S. L., Fuchs, C. A., Kimble, H. J. and van Loock, P. (2001), 'Quantum versus classical domains for teleportation with continuous variables', *Phys. Rev. A* **64**, 022321.

Braunstein, S. L. and Kimble, H. J. (1998), 'Teleportation of continuous quantum variables', *Phys. Rev. Lett.* **80**, 869–872.

Braunstein, S. L. and van Loock, P. (2005), 'Quantum information with continuous variables', *Reviews of Modern Physics* **77**, 513–577.

Cerf, N. J., Lévy, M. and Assche, G. V. (2001), 'Quantum distribution of gaussian keys using squeezed states', *Phys. Rev. A* **63**, 052311.

Cohen-Tannoudji, C., Diu, B. and Laloe, F. (2006), *Quantum Mechanics*, Wiley-VCH Verlag GmbH.

Diffie, W. and Hellman, M. (2006), 'New directions in cryptography', *IEEE Trans. Inf. Theor.* **22**(6), 644–654.

Eberle, T., Händchen, V. and Schnabel, R. (2013), 'Stable control of 10 db two-mode squeezed vacuum states of light', *Opt. Express* **21**(9), 11546–11553.

Einstein, A., Podolsky, B. and Rosen, N. (1935), 'Can quantum-mechanical description of physical reality be considered complete?', *Phys. Rev.* **47**, 777–780.

Eisert, J. and Plenio, M. B. (2003), 'Introduction to the basics of entanglement theory in continuous-variable systems', *International Journal of Quantum Information* **01**(04), 479–506.

Ekert, A. K. (1991), 'Quantum cryptography based on bell's theorem', *Phys. Rev. Lett.* **67**, 661–663.

Elser, D., Bartley, T., Heim, B., Wittmann, C., Sych, D. and Leuchs, G. (2009), 'Feasibility of free space quantum key distribution with coherent polarization states', *New Journal of Physics* **11**(4), 045014.

Furusawa, A., Sørensen, J. L., Braunstein, S. L., Fuchs, C. A., Kimble, H. J. and Polzik, E. S. (1998), 'Unconditional quantum teleportation', *Science* **282**(5389), 706–709.

Galindo, A., Pascual, P., Garcia, J. and Alvarez-Gaume, L. (2012), *Quantum Mechanics I*, Theoretical and Mathematical Physics, Springer London, Limited.

Gelfand, I. and Vilenkin, N. (1964), *Generalized Functions: Vol.: 4. : Applications of Harmonic Analysis*, Academic Press.

Giedke, G., Duan, L.-M., Cirac, J. I. and Zoller, P. (2001), 'Distillability criterion for all bipartite gaussian states', *Quantum Information and Computation* **1**(3), 79–86.

Gisin, N., Ribordy, G., Tittel, W. and Zbinden, H. (2002), 'Quantum cryptography', *Rev. Mod. Phys.* **74**, 145–195.

Glauber, R. J. (1963), 'The quantum theory of optical coherence', *Phys. Rev.* **130**, 2529–2539.

Gordon, G. and Rigolin, G. (2010), 'Quantum cryptography using partially entangled states', *Optics Communications* **283**(1), 184 – 188.

Gottesman, D. and Preskill, J. (2001), 'Secure quantum key distribution using squeezed states', *Phys. Rev. A* **63**, 022309.

Griffiths, D. (2011), *Mecânica Quântica*, Pearson Prentice Hall.

Grosshans, F. and Cerf, N. J. (2004), 'Continuous-variable quantum cryptography is secure against non-gaussian attacks', *Phys. Rev. Lett.* **92**, 047905.

Grosshans, F. and Grangier, P. (2002), 'Continuous variable quantum cryptography using coherent states', *Phys. Rev. Lett.* **88**, 057902.

Grosshans, F., Van Assche, G., Wenger, J., Brouri, R., Cerf, N. J. and Grangier, P. (2003), 'Quantum key distribution using gaussian-modulated coherent states', *Nature* **421**, 042331.

Halliday, T. (1983), *Animal Behaviour*, number v. 2, Cambridge University Press.

Hankerson, D., Harris, G. and Johnson, P. (2003), *Introduction to Information Theory and Data Compression, Second Edition*, Applied Mathematics, Taylor & Francis.

Heid, M. and Lütkenhaus, N. (2006), 'Efficiency of coherent-state quantum cryptography in the presence of loss: Influence of realistic error correction', *Phys. Rev. A* **73**, 052316.

Heid, M. and Lütkenhaus, N. (2007), 'Security of coherent-state quantum cryptography in the presence of gaussian noise', *Phys. Rev. A* **76**, 022313.

Hillery, M. (2000), 'Quantum cryptography with squeezed states', *Phys. Rev. A* **61**, 022309.

Hirano, T., Yamanaka, H., Ashikaga, M., Konishi, T. and Namiki, R. (2003), 'Quantum cryptography using pulsed homodyne detection', *Phys. Rev. A* **68**, 042331.

Houston, S. (2004), *The First Writing: Script Invention as History and Process*, Cambridge University Press.

Iblisdir, S., Van Assche, G. and Cerf, N. J. (2004), 'Security of quantum key distribution with coherent states and homodyne detection', *Phys. Rev. Lett.* **93**, 170502.

Ide, T., Hofmann, H. F., Furusawa, A. and Kobayashi, T. (2002), 'Gain tuning and fidelity in continuous-variable quantum teleportation', *Phys. Rev. A* **65**, 062303.

Jouguet, P., Kunz-Jacques, S., Leverrier, A., Grangier, P. and Diamanti, E. (2002), 'Quantum key distribution using gaussian-modulated coherent states', *Nature* **7**, 378–381.

Julien, N. (2008), Quantum Information with Optical Continuous Variables, Doutorado, Université Libre de Bruxelles.

Klauder, J. R. (1960), 'The action option and a feynman quantization of spinor fields in terms of ordinary c-numbers', *Annals of Physics* **11**(2), 123 – 168.

Kogias, I., Ragy, S. and Adesso, G. (2014), 'Continuous-variable versus hybrid schemes for quantum teleportation of gaussian states', *Phys. Rev. A* **89**, 052324.

Kollmitzer, C. and Pivk, M. (2010), *Applied Quantum Cryptography*, Lecture Notes in Physics, Springer.

Lee, N., Benichi, H., Takeno, Y., Takeda, S., Webb, J., Huntington, E. and Furusawa, A. (2011), 'Teleportation of nonclassical wave packets of light', *Science* **332**(6027), 330–333.

Leonhardt, U. (1997), *Measuring the Quantum State of Light*, Cambridge Studies in Modern Optics, Cambridge University Press.

Leverrier, A. and Grangier, P. (2009), 'Unconditional security proof of long-distance continuous-variable quantum key distribution with discrete modulation', *Phys. Rev. Lett.* **102**, 180504.

Leverrier, A. and Grangier, P. (2011), 'Continuous-variable quantum-key-distribution protocols with a non-gaussian modulation', *Phys. Rev. A* **83**, 042312.

Lo, H.-K., Ma, X. and Chen, K. (2005), 'Decoy state quantum key distribution', *Phys. Rev. Lett.* **94**, 230504.

Lorenz, S., Korolkova, N. and Leuchs, G. (2004), 'Continuous-variable quantum key distribution using polarization encoding and post selection', *Applied Physics B* **79**(3), 273–277.

Luiz, F. S. and Rigolin, G. (2013), 'Optimal continuous variable quantum teleportation protocol for realistic settings', *arXiv:1309.3508 v1[quant-ph]* .

Luiz, F. S. and Rigolin, G. (2014), 'Teleportation-based continuous variable quantum cryptography', *arXiv:1408.5012 v1 [quant-ph]* .

Martinez, F., Moreira, C.G.T.A. and, S. C. and Tengan, E. (2010), *Teoria dos números: um passeio com primos e outros números familiares pelo mundo inteiro*, IMPA.

Mišta, L., Filip, R. and Furusawa, A. (2010), 'Continuous-variable teleportation of a negative wigner function', *Phys. Rev. A* **82**, 012322.

Navascués, M., Grosshans, F. and Acín, A. (2006), 'Optimality of gaussian attacks in continuous-variable quantum cryptography', *Phys. Rev. Lett.* **97**, 190502.

Nielsen, M. A. and Chuang, I. L. (2004), *Quantum Computation and Quantum Information*, Cambridge University Press, Cambridge, MA, USA.

Olmschenk, S., Matsukevich, D. N., Maunz, P., Hayes, D., Duan, L.-M. and Monroe, C. (2009), 'Quantum teleportation between distant matter qubits', *Science* **323**(5913), 486–489.

Orszag, M. (2007), *Quantum Optics: Including Noise Reduction, Trapped Ions, Quantum Trajectories, and Decoherence*, Springer.

Paul, H. (2004), *Introduction to Quantum Optics: From Light Quanta to Quantum Teleportation*, Cambridge University Press.

Pfaff, W., Hensen, B., Bernien, H., van Dam, S. B., Blok, M. S., Taminiau, T. H., Tiggelman, M. J., Schouten, R. N., Markham, M., Twitchen, D. J. and Hanson, R. (2014), 'Unconditional quantum teleportation between distant solid-state quantum bits', *Science* .

Pierce, J. (2012), *An Introduction to Information Theory: Symbols, Signals and Noise*, Dover Books on Mathematics, Dover Publications.

Pirandola, S. and Mancini, S. (2006), 'Quantum teleportation with continuous variables: A survey', *Laser Physics* **16**(10), 1418–1438.

Polkinghorne, R. E. S. and Ralph, T. C. (1999), 'Continuous variable entanglement swapping', *Phys. Rev. Lett.* **83**, 2095–2099.

Ralph, T. C. (1999), 'Continuous variable quantum cryptography', *Phys. Rev. A* **61**, 010303.

Ralph, T. C., Gilchrist, A., Milburn, G. J., Munro, W. J. and Glancy, S. (2003), 'Quantum computation with optical coherent states', *Phys. Rev. A* **68**, 042319.

Ralph, T. C. and Lam, P. K. (1998), 'Teleportation with bright squeezed light', *Phys. Rev. Lett.* **81**, 5668–5671.

Reid, M. D. (2000), 'Quantum cryptography with a predetermined key, using continuous-variable einstein-podolsky-rosen correlations', *Phys. Rev. A* **62**, 062308.

Reza, F. (2012), *An Introduction to Information Theory*, Dover Books on Mathematics, Dover Publications.

Rigolin, G. (2009), 'Unity fidelity multiple teleportation using partially entangled states', *Journal of Physics B: Atomic, Molecular and Optical Physics* **42**(23), 235504.

Rigolin, G. and Escobar, C. O. (2004), 'Lower bounds on the entanglement of formation for general gaussian states', *Phys. Rev. A* **69**, 012307.

Rigolin, G. G. (2005), Estados Quânticos Emaranhados, Doutorado, Unicamp.

Rivest, R. L., Shamir, A. and Adleman, L. (1978), 'A method for obtaining digital signatures and public-key cryptosystems', *Commun. ACM* **21**(2), 120–126.

Rogers, D. (2010), *Broadband Quantum Cryptography*, Synthesis lectures on quantum computing, Morgan & Claypool Publishers.

Rosenberg, J. (2004), A selective history of the Stone-von Neumann theorem, *in* 'Operator algebras, quantization, and noncommutative geometry', Vol. 365 of *Contemp. Math.*, Amer. Math. Soc., Providence, RI, pp. 331–353.

Scarani, V., Acín, A., Ribordy, G. and Gisin, N. (2004), 'Quantum cryptography protocols robust against photon number splitting attacks for weak laser pulse implementations', *Phys. Rev. Lett.* **92**, 057901.

Scarani, V., Bechmann-Pasquinucci, H., Cerf, N. J., Dušek, M., Lütkenhaus, N. and Peev, M. (2009), 'The security of practical quantum key distribution', *Rev. Mod. Phys.* **81**, 1301–1350.

Schleich, W. (2001), *Quantum Optics in Phase Space*, Wiley-VCH.

Schrödinger, E. (1926), 'Der stetige Übergang von der mikro- zur makromechanik', *Naturwissenschaften* **14**, 664–666.

Schrödinger, E. (1935), 'Discussion of probability relations between separated systems', *Mathematical Proceedings of the Cambridge Philosophical Society* **31**, 555–563.

Schumaker, B. L. and Caves, C. M. (1985), 'New formalism for two-photon quantum optics. ii. mathematical foundation and compact notation', *Phys. Rev. A* **31**, 3093–3111.

Scully, M. and Zubairy, S. (1997), *Quantum Optics*, Cambridge University Press.

Shannon, C. and Weaver, W. (1949), *The Mathematical Theory of Communication*, Urbana.

Shor, P. (1994), Algorithms for quantum computation: discrete logarithms and factoring, *in* 'Foundations of Computer Science, 1994 Proceedings., 35th Annual Symposium on', pp. 124–134.

Silberhorn, C., Ralph, T. C., Lütkenhaus, N. and Leuchs, G. (2002), 'Continuous variable quantum cryptography: Beating the 3 db loss limit', *Phys. Rev. Lett.* **89**, 167901.

Steiner, F. (1988), 'Schrödinger's discovery of coherente states', *Physica B+C* **151**(1-2), 323–326.

Sudarshan, E. C. G. (1963), 'Equivalence of semiclassical and quantum mechanical descriptions of statistical light beams', *Phys. Rev. Lett.* **10**, 277–279.

Sych, D. and Leuchs, G. (2010), 'Coherent state quantum key distribution with multi letter phase-shift keying', *New Journal of Physics* **12**(5), 053019.

Toledo Piza, A. (2009), *Mecânica Quântica*, Edusp.

Vaidman, L. (1994), 'Teleportation of quantum states', *Phys. Rev. A* **49**, 1473–1476.

Van Assche, G. (2006), *Quantum Cryptography and Secret-Key Distillation*, Cambridge University Press.

van Loock, P. and Braunstein, S. L. (1999), 'Unconditional teleportation of continuous-variable entanglement', *Phys. Rev. A* **61**, 010302.

Vernam, G. S. (1926), 'Cipher printing telegraph systems for secret wire and radio telegraphic communications', *American Institute of Electrical Engineers, Transactions of the* **XLV**, 295–301.

Walls, D. and Milburn, G. (2008), *Quantum Optics*, SpringerLink: Springer e-Books, Springer.

Wang, X.-B., Hiroshima, T., Tomita, A. and Hayashi, M. (2007), 'Quantum information with gaussian states', *Physics Reports* **448**(1–4), 1 – 111.

Waterhouse, W., Brinkhuis, J., Clarke, A., Gauss, C. and Greiter, C. (1986), *Disquisitiones Arithmeticae*, Springer New York.

Weedbrook, C., Pirandola, S., García-Patrón, R., Cerf, N. J., Ralph, T. C., Shapiro, J. H. and Lloyd, S. (2012), 'Gaussian quantum information', *Rev. Mod. Phys.* **84**, 621–669.

Wootters, W. K. and Zurek, W. H. (1982), 'A single quantum cannot be cloned', *Nature* **299**(5886), 802–803.

Yonezawa, H., Furusawa, A. and van Loock, P. (2007), 'Sequential quantum teleportation of optical coherent states', *Phys. Rev. A* **76**, 032305.

Zhang, T. C., Goh, K. W., Chou, C. W., Lodahl, P. and Kimble, H. J. (2003), 'Quantum teleportation of light beams', *Phys. Rev. A* **67**, 033802.