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

Distribuição Quântica de Chave Secreta Utilizando Mapas de Shannon-Kotel'nikov

Francisco Revson Fernandes Pereira

Área de Conhecimento: Processamento da Informação

Orientador:
Francisco Marcos de Assis

Campina Grande, Paraíba, Brasil

Distribuição Quântica de Chave Secreta Utilizando Mapas de Shannon-Kotel'nikov

Francisco Revson Fernandes Pereira

Dissertação de Mestrado apresentada à Coordenação do Curso de Pós-Gradução em Engenharia Elétrica da Universidade Federal de Campina Grande, como parte dos requisitos necessários para obtenção do título de mestre em Engenharia Elétrica.

Francisco Revson Fernandes Pereira

Aluno

Francisco Marcos de Assis

Orientador

Campina Grande, Paraíba, Brasil

Fevereiro de 2016

FICHA CATALOGRÁFICA ELABORADA PELA BIBLIOTECA CENTRAL DA UFCG

P436d Pereira, Francisco Revson Fernandes.
Distribuição quântica de chave secreta utilizando mapas de shannon-kotel'nikov / Francisco Revson Fernandes Pereira. – Campina Grande, 2016.
85 f. : il. color.

Dissertação (Mestrado em Engenharia Elétrica) – Universidade Federal de Campina Grande, Centro de Engenharia Elétrica e Informática, 2016.
"Orientação: Prof. Dr. Francisco Marcos de Assis".
Referências.

1 Distribuição Quântica - Chave Secreta. 2. Adaptativo. 3. Shannon-Kotel'nikov - Mapas. 4. Variáveis Contínuas. I. Assis, Francisco Marcos de. II. Título.

CDU 621:530.145 (043)

"DISTRIBUIÇÃO QUÂNTICA DE CHAVE SECRETA UTILIZANDO MAPAS DE SHANNON-KOTELNIKOV "

FRANCISCO REVSON FERNANDES PEREIRA

DISSERTAÇÃO APROVADA EM 24/02/2016

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

HELDER ALVES PEREIRA, Dr., UFCG
Examinador(a)

DANIEVERTON MORETTI, Dr., UFCG
Examinador(a)

REX ANTONIO DA COSTA MEDEIROS, Dr., UFRN
Examinador(a)

CAMPINA GRANDE - PB

Este trabalho é dedicado à minha família

Agradecimentos

Os agradecimentos deste trabalho são direcionados:

- A Deus, pela força e perseverança, pela capacidade e sabedoria;
- Ao professor Francisco Marcos, pela orientação, confiança, por estar sempre à disposição para qualquer problema que tiver e, além de tudo, pelos conselhos sobre a vida pessoal e profissional que eu levarei para sempre;
- Ao professor Danieverton Moretti, por ter me ajudado a iniciar na grande área da Mecânica Quântica, área esta que me apaixonei desde o início, e por estar sempre à disposição para ser o amigo que é;
- À Juliana Martins, por me ajudar na parte da estimação da informação mútua;
- À minha família, pelo apoio, estímulo e por nunca desistirem de mim, não apenas durante esses cinco anos e meio, mas durante toda a minha vida;
- A todos os amigos e colegas, em particular a Dudz, Lolo, Tantan, Jagra, Roiben e Serafa por me mostrarem que, independentemente da situação e do momento, sempre é possível ser feliz feito a gota serena;
- A todos os professores e a todas as pessoas anônimas que, de forma direta ou indireta, contribuíram para a realização deste trabalho.
- Ao CNPQ, CAPES e ao projeto QUANTA/RENASIC/FINEP por financiarem este trabalho de pesquisa.

"Se soubéssemos o que estamos fazendo, não se chamaria de pesquisa."
(Albert Einstein, 1879 - 1955)

Resumo

Na presente dissertação, são apresentadas contribuições à área de distribuição quântica de chave secreta. Essas contribuições utilizaram as teorias de mapas de Shannon-Kotel'nikov e de variáveis contínuas em mecânica quântica para dar síntese ao protocolo proposto e analisado. Nele é utilizado estados comprimidos bimodais em adição a curvas em camada de toro. Em nosso protocolo, que é adaptativo quanto ao nível de ruído do canal, demonstramos que a informação mútua entre Alice e Bob é maior que entre Ela e Eva. Com isso, desenvolvemos um método capaz de gerar e transmitir uma chave secreta mesmo quando o nível de ruído do canal for superior aos valores aceitos atualmente, manipulando apenas parâmetros relacionados com os ruídos das quadraturas. Para maiores valores de compressão e em canais mais ruidosos, a chave produzida ainda se mantêm secreta quando Eva utiliza o ataque *beam-splitting*.

Palavras-chaves: adaptativo, distribuição quântica de chave secreta, mapas de Shannon-Kotel'nikov, variáveis contínuas.

Abstract

In this thesis, the contributions are done in the quantum key distribution's area. These contributions have used the theories of Shannon-Kotelnikov mapping and continuous variables in quantum mechanics to give synthesis to the proposed and analyzed protocol. It is used bimodal squeezed states in addition to curves in flat torus. In our protocol, which is adaptive in term of the channel noise level, was demonstrated that the mutual information between Alice and Bob is greater than between Alice and Eve. Therefore, we developed a method capable to generate and transmit a secret key even when the channel noise level is higher than the values currently accepted, by manipulating only parameters related to the variance of the quadrature. For higher compression values and more noisy channels, the produced key still remain secret when Eva uses the beam-sppliting attack.

Keywords: adaptive, continuous variable, quantum key distribution, Shannon-Kotelnikov mapping.

Lista de ilustrações

Lista de tabelas

Lista de abreviaturas e siglas

AM	*Analog Modulation*
AWGN	*Additive White Gaussian Noise*
FDP	*Função Densidade de Probabilidade*
FM	*Frequency Modulation*
LDPC	*Low Density Parity Check*
PPM	*Pulse Position Modulation*
QBER	*Taxa de Erro de Bit Quântico*
QKD	*Quantum Key Distribution*

Lista de símbolos

$\|\psi\rangle$	Vetor complexo do espaço de Hilbert
$\langle\psi\|$	Vetor complexo do espaço de Hilbert dual a $\|\psi\rangle$
ρ	Matriz densidade
$\hat{\mathcal{H}}$	Hamiltoniano do sistema
$\mathcal{I}$	Operador identidade
$\{M_m\}$	Conjunto de operadores de medida
$\hbar$	Constante de Plank dividida por 2π
ΔA	Desvio padrão de A
$\mathbf{\Sigma}_A$	Matriz de covariância do observável A
k_B	Constante de Boltzmann
$\mathbf{E}$	Campo elétrico
$\mathbf{B}$	Campo magnético
c	Velocidade da luz no vácuo
ϵ_0	Permissividade dielétrica do vácuo
μ_0	Permeabilidade do vácuo
$\mathbf{k}$	Vetor de onda
Z	Função de partição
$\hat{a}$	Operador de aniquilação
$\hat{a}^\dagger$	Operador de criação
$\hat{D}(\alpha)$	Operador de deslocamento
$\hat{S}(\xi)$	Operador de compressão (ou de *squeeze*)
$\hat{S}_2(\xi)$	Operador de compressão bimodal
r	Fator de compressão

$\|\alpha\rangle$	Estado coerente
$\|\xi\rangle$	Estado comprimido
Enc	Função de cifragem
Dec	Função de decifragem
I	Informação mútua
$\mathcal{G}$	Classe de funções $universal_2$
m	Símbolo gerado pela fonte
$\mathbf{s}_m$	Vetor transmitido pelo canal
$\mathbf{r}$	Vetor recebido pelo receptor
ϵ	Erro médio quadrático
S	Fator de alongamento
$\mathbf{\Phi_c}$	Função de parametrização de um toro planar

Sumário

1 Introdução

A criptografia é o estudo de técnicas de codificação de mensagens voltadas à proteção da informação contida nela [1, 2, 3]. O uso conhecido mais antigo de tais técnicas foi encontrado no Egito antigo por volta de 1900 A.C. em hieróglifos esculpidos em monumentos, mas com o objetivo voltado para os mistérios religiosos que cultivavam [4]. O começo do uso da criptografia para objetivos militares só seria realizado pelos gregos antigos e resultou na criação da cifra de César [4]. Depois disso, a criptografia foi difundida e mais apreciada por diversos povos, sendo creditado aos árabes a documentação sistemática de diversos métodos de criptografia.

Mesmo a criptografia tendo uma longa e complexa história, seu desenvolvimento pode ser classificado como supérfluo comparado com aquele feito a partir do século 19 [4]. Métodos sistemáticos de quebra de cifras foram criados e incentivados, diferentes daqueles já existentes que se baseavam em técnicas de força bruta. Em 1917 [5], Gilbert Vernam propôs uma cifra de teletipo em que uma chave previamente preparada, mantida em fita de papel, é combinada caractere a caractere com a mensagem de texto em claro para produzir o texto cifrado. Isto levou ao desenvolvimento de dispositivos eletromecânicos como máquinas de cifra. Métodos matemáticos foram desenvolvidos no período anterior à Segunda Guerra Mundial (particularmente na aplicação de técnicas estatísticas para criptoanálise, desenvolvimento de cifras de William F. Friedman e na ruptura inicial da versão do Enigma do Exército Alemão por Marian Rejewski [6]).

A criptografia moderna, que é conhecida nos dias de hoje, é realizada pelo uso de algoritmos que utilizam chaves para cifrar e decifrar a informação que se deseja estar em sigilo. Essas chaves transformam a mensagem em dados sem sentido, para um agente que não deve ter conhecimento da mesma, no processo de cifragem, e a retorna ao formato inicial no processo de descriptografia. Em geral, chaves maiores garantem uma maior dificuldade de quebra do código[1].

Claude Shannon é creditado o pai da criptografia matemática pelo seu trabalho realizado durante a segunda guerra mundial sobre a segurança de sistema de comunicações. O seu artigo publicado em 1949 [7] influenciou pesquisas em criptografia nos anos 70, como o desenvolvimento do sistema criptográfico de chave pública [8].

A criptografia de chave pública foi criada em 1976 por M. E. Hellman e W. Diffie [8]. Esse método criptográfico consiste em utilizar um par de chaves: uma pública e uma privada. A chave pública é distribuída a todas as partes que devem transmitir a mensa-

[1] Quebra do código significa a obtenção, por um agente não autêntico, da informação criptografada sem que o mesmo tenha a chave de decifragem.

gem criptografada, enquanto a chave privada deve ser conhecida apenas por quem está recebendo a mensagem. Neste algoritmo, uma mensagem criptografada com uma chave pública só pode ser descriptografada com a chave privada.

Existe também outro método criptográfico bastante conhecido e utilizado, que é a criptografia de chave secreta ou simétrica [1, 3]. Esse processo criptográfico é mais simples que o anterior, pois utiliza apenas uma chave para as partes de criptografia e descriptografia. A chave, na prática, representa um segredo, partilhado entre duas ou mais partes, que podem ser usadas para manter um canal confidencial de informação. Usa-se uma única chave, partilhada por ambos os interlocutores, na premissa de que esta é conhecida apenas por eles. O principal problema deste método é a garantia da afirmação anterior, porém isto pode ser feito com a utilização da criptografia quântica [9].

O uso da criptografia quântica ou, mais especificamente, da Distribuição Quântica de Chaves (QKD, do inglês *Quantum Key Distribution*) tem como objetivo a distribuição de uma chave secreta entre duas partes (Alice e Bob) para fins criptográficos. A segurança do processo não reside em hipóteses computacionais, mas em fundamentos da mecânica quântica, como a impossibilidade de se realizar cópias perfeitas de estados quânticos não ortogonais [10]. Mais de duas décadas após o protocolo pioneiro BB84 [11], vários protocolos para QKD foram implementados com sucesso, tanto em laboratório como em aplicações comerciais [12].

Atualmente, os protocolos para QKD podem ser implementados usando variáveis discretas ou contínuas [10]. Nos protocolos com variáveis discretas, a informação é codificada usualmente na polarização ou na fase de fótons únicos [10]. Por outro lado, nos protocolos com variáveis contínuas, a informação é codificada nas amplitudes de quadratura do campo eletromagnético quantizado [13, 14]. Uma das vantagens da abordagem com variáveis contínuas é que ela permite implementações mais simples, usando componentes ópticos convencionais utilizados em transmissões em fibras ópticas [15].

No paradigma clássico, modulações não lineares nos sistemas analógicos têm a vantagem de permitir uma diminuição no erro médio quadrático sem a necessidade de aumentar a potência do sinal transmitido [16]. Uma desvantagem desses esquemas de modulação é a sensibilidade a níveis de ruído que ultrapassam um determinado limiar [17]. Na ocorrência de tais eventos, verifica-se uma distorção extrema no sinal demodulado, ou até mesmo a perda total do sinal. A grande distorção que pode ocorrer durante a demodulação de sistemas não lineares entretanto, pode ser útil, em sistemas QKD, para facilitar a identificação da presença de um espião. Esta ideia foi explorada durante a pesquisa realizada.

Com base no que foi exposto, propõe-se neste trabalho uma variação no protocolo de Weedbrook, et al. [18] aplicando-se os conceitos de modulação não linear (Mapas de Shannon-Kotel'nikov) apresentados em Wozencraft [16]. A ideia é mapear uma variá-

vel aleatória gaussiana em uma curva não linear em um espaço quadrimensional, sendo os pontos desza curva correspondentes aos estados coerentes a serem preparados. Desta forma, a estrutura da curva é usada para detectar a presença do espião e para melhorar a correlação entre as variáveis de Alice e Bob a serem reconciliadas.

Uma análise bibliográfica construída neste trabalho é feita e mostra que o estudo e a pesquisa relacionados com este trabalho são novas e de interesse à comunidade científica. Além de propor o método, é apresentado uma forma de detecção de espião no canal de comunicação com a utilização da probabilidade de anomalia. Por fim, os pontos relevantes que serão feitos no restante do mestrado são apresentados.

1.1 Justificativa e Relevância

A transmissão de mensagens para as partes autênticas (Alice e Bob) com a impossibilidade da ação de uma espiã (Eva) na obtenção da informação contida nela é imprescindível em diversos sistemas de comunicação, tal como sistemas bancários e de troca de e-mail [3]. O uso da distribuição quântica de chave está cada vez mais sendo estudado e utilizado na prática para que esta segurança seja garantida [10]. Diversas formulações para a QKD foram criadas e apresentadas, porém nenhuma foi construída com a utilização de formas não lineares de geração da chave, tal como a modulação não linear.

O desenvolvimento deste trabalho contempla a investigação do uso de esquemas de modulação não linear na preparação de estados quânticos utilizados para distribuição quântica de chaves secretas. Isso será feito com a construção de formas de comparação do protocolo proposto de troca de chave com os protocolos mais conhecidos e aceitos na literatura, mostrando as vantagens e as desvantagens do mesmo sobre diversas circunstâncias, lembrando que a implementação experimental do protocolo proposto é tão viável quanto os já existentes, pois utiliza os mesmos dispositivos ópticos utilizados em telecomunicações.

1.2 Objetivos

Esta dissertação tem como objetivo geral contribuir para o desenvolvimento de técnicas para QKD. O trabalho tem como foco principal a apresentação e análise do protocolo proposto para QKD com a utilização de modulação não linear. O estudo e análise do protocolo será feito sobre as vertentes de comparação com os métodos já existentes. Para alcançar o objetivo principal, alguns objetivos específicos foram contemplados:

1. Revisão bibliográfica de QKD com as metas de solidificar o conceito, ter conheci-

mento do estado da arte atual e obter uma base de comparação para o protocolo proposto;

2. Estudo e análise do método de modulação não linear para que este seja utilizado de forma eficiente e viável no trabalho;

3. Proposição, simulação e aprimoramento do protocolo de QKD utilizando modulação não linear;

4. Análise do protocolo proposto para QKD através da integração de um modelo físico para o canal quântico;

5. Comparação dos resultados obtidos com os mais relevantes existentes e aceitos na literatura de protocolos de QKD.

1.3 Organização do texto

Os três capítulos seguintes, Cap. 2, 3 e 4, fundamentam a base teórica necessária para o entendimento do Cap. 5, no qual é apresentado e analisado o protocolo criado. Em suma, no Capítulo 2 são apresentados os conceitos básicos de mecânica quântica através da exposição dos postulados, assim como uma breve discussão a respeito de óptica quântica. No Capítulo 3 é apresentada a motivação para a criação dos protocolos QKD, tanto quanto uma revisão dos trabalhos existentes na literatura, com ênfase nos aspectos que os diferenciam. No Capítulo 4, uma descrição matemática de esquemas de modulação linear e não linear é feita, de forma a ser possível usá-los no que se segue no trabalho. No Capítulo 5 é exposta a contribuição do trabalho, que é feita pela exibição do protocolo proposto e a análise e comparação dos resultados obtidos com os já existentes. No Capítulo 6 é mostrado uma breve síntese do trabalho e são manifestadas ideias para possíveis trabalhos futuros.

1.4 Lista de Publicações

Durante o desenvolvimento desse trabalho de dissertação foi produzido três publicações. Duas no XXXIII Simpósio Brasileiro de Telecomunicações intituladas “Distribuição Quântica de Chave Utilizando Modulação Não Linear” [19] e “Protocolo para Autenticação Quântica de Mensagens Clássicas Utilizando Variáveis Contínuas” [20] e uma no V Workshop-Escola em Computação e Informação Quântica com o título “Modulação Não-Linear de Estados Coerentes” [21].

2 Fundamentos de Mecânica e Óptica Quânticas

Nesse capítulo será apresentada uma introdução bastante resumida sobre os fundamentos da mecânica e da óptica quânticas. Caso o leitor já tenha conhecimento do assunto, ele pode seguir para os capítulos seguintes. Em particular, para o Cap. 5, no qual se encontra a contribuição deste trabalho.

2.1 Elementos de Mecânica Quântica

Será apresentado um brevíssimo resumo de Mecânica Quântica necessário para que se tenha um *background* mínimo para o entendimento do restante do trabalho.

2.1.1 Os Postulados da Mecânica Quântica

A Mecânica Quântica é construída sobre quatro postulados [22]:

- **Postulado 1** - Todo sistema físico tem a ele associado um espaço vetorial complexo chamado de espaço de Hilbert. Os elementos do espaço de Hilbert são vetores complexos $|\psi\rangle$, chamados de kets, e representam o estado físico do sistema. O complexo conjugado de um ket é chamado de bra, representado por $\langle\psi|$. Como esses elementos são vetores, então eles podem ser decompostos em uma base, por exemplo, considere a base $\mathcal{B} = \{|b_1\rangle, \cdots, |b_n\rangle\}$ de um espaço de Hilbert n dimensional, o vetor $|\psi\rangle$ é decomposto nessa base da seguinte forma

$$|\psi\rangle = b_1 |b_1\rangle + \cdots + b_n |b_n\rangle, \tag{2.1}$$

  onde $b_i = \langle b_i | \psi\rangle$, para $i = 1, \cdots, n$, e $\sum_{i=1}^{n} |b_i|^2 = 1$. Essa noção de decomposição pode ser expandida para espaços de Hilbert com espectro contínuo, como será mostrado posteriormente neste capítulo.

- **Postulado 2** - A evolução temporal de um sistema quântico isolado, ou seja, que não interage com sua vizinhança[1], dá-se através de transformações unitárias:

$$|\psi(t)\rangle = \hat{U}(t) |\psi(0)\rangle, \tag{2.2}$$

[1] Quando há a influência de um ambiente, tal como um reservatório térmico, o hamiltoniano $\hat{\mathcal{H}}$ pode conter termos relacionados a interações entre partículas e/ou campos, por exemplo. Assim, o sistema não será isolado, de fato.

onde $\hat{U}^\dagger(t)\hat{U}(t) = \mathcal{I}$, sendo $\mathcal{I}$ a matriz identidade. A relação do operador $\hat{U}$[2] com o hamiltoniano $\hat{\mathcal{H}}$ do sistema é:

$$\hat{U}(t) = \exp\Big(-\frac{i}{\hbar}\hat{\mathcal{H}}t\Big). \tag{2.3}$$

Fisicamente, transformações unitárias representam processos temporalmente reversíveis. De fato, aplicando-se $\hat{U}^\dagger(t)$ pela esquerda nos dois lados da Eq. 2.2 obtém-se

$$|\psi(0)\rangle = \hat{U}^\dagger(t)\,|\psi(t)\rangle\,. \tag{2.4}$$

Uma outra propriedade importante das transformações unitárias é a conservação do produto escalar, ou seja,

$$\langle\psi(0)|\,\hat{U}^\dagger\hat{U}\,|\psi(0)\rangle = \langle\psi(0)\,|\psi(0)\rangle = \langle\psi(t)\,|\psi(t)\rangle\,. \tag{2.5}$$

- **Postulado 3** - Medidas em Mecânica Quântica são representadas por um conjunto de operadores de medidas $\{\hat{M}_m\}$, onde o índice m refere-se aos possíveis resultados da medida. A probabilidade de que o resultado m seja encontrado em uma medida feita em um sistema quântico preparado no estado $|\psi\rangle$ é dada por

$$p_M(m) = \langle\psi|\,\hat{M}_m^\dagger\hat{M}_m\,|\psi\rangle \tag{2.6}$$

e o estado do sistema, após a medida com resultado m, será:

$$|\psi_m\rangle = \frac{\hat{M}_m}{\sqrt{p_M(m)}}\,|\psi\rangle\,. \tag{2.7}$$

A normalização das probabilidades, $\sum_m p_M(m) = 1$, a hipótese de que $\langle\psi\,|\psi\rangle = 1$ e a Eq. (2.6) implicam na relação de completitude

$$\sum_m \hat{M}_m^\dagger\hat{M}_m = \mathcal{I}. \tag{2.8}$$

- **Postulado 4** - Os elementos do espaço de Hilbert de um sistema quântico composto AB é formado pelo produto tensorial dos kets dos espaços de Hilbert dos sistemas individuais:

$$|\psi_{AB}\rangle = |\psi_A\rangle \otimes |\psi_B\rangle\,. \tag{2.9}$$

Esta regra pode ser estendida para N sistemas individuais.

[2] Neste trabalho será utilizada a notação de se colocar um "chapéu" sobre as quantidades que são operadores, de modo que $\hat{x}$ representa o operador da quantidade física x.

2.1.2 Princípio de Indeterminação

O princípio da indeterminação de Heisenberg consiste num enunciado da Mecânica Quântica, formulado inicialmente em 1927 por Werner Heisenberg [23], impondo restrições à precisão com que se podem efetuar medidas simultâneas de uma classe de pares de observáveis.

Em Mecânica Quântica, observáveis, tais como posição e *momentum*, são representados por operadores hermitianos. Quando se considera pares de observáveis, uma das quantidades mais importantes é o comutador. Para um par de observáveis A e B, define-se seu comutador como sendo

$$[\hat{A}, \hat{B}] = \hat{A}\hat{B} - \hat{B}\hat{A}. \tag{2.10}$$

Com essa definição, é possível mostrar que a relação de comutação entre a posição e o *momentum* é [24]

$$[\hat{x}, \hat{p}_x] = i\hbar. \tag{2.11}$$

O significado físico é que operadores que não comutam entre si não podem ser medidos com qualquer precisão simultaneamente, sempre ocorrendo um erro na medida dos observáveis.

A forma geral mais comum do princípio de indeterminação é a relação de indeterminação de Robertson [25]. Para um operador hermitiano arbitrário $\hat{O}$, associa-se o desvio padrão como sendo

$$\Delta_O = \sqrt{\langle \hat{O}^2 \rangle - \langle \hat{O} \rangle^2}, \tag{2.12}$$

onde $\langle \hat{O} \rangle$ denota o valor médio[3]. Para um par de operadores $\hat{A}$ e $\hat{B}$, a relação de indeterminação de Robertson é dada por

$$\Delta_A \Delta_B \geqslant \frac{1}{2} |\langle [\hat{A}, \hat{B}] \rangle|. \tag{2.13}$$

Outra expressão para o princípio de indeterminação é a relação de indeterminação de Schrödinger, que é

$$\Delta_A^2 \Delta_B^2 \geqslant \frac{1}{2} \{ |\langle \{\hat{A}, \hat{B}\} \rangle - \langle \hat{A} \rangle \langle \hat{B} \rangle|^2 + |\langle [\hat{A}, \hat{B}] \rangle|^2 \}, \tag{2.14}$$

[3] Também é usado neste trabalho $\overline{O}$ para denotar o valor médio do operador $\hat{O}$

em que o anticomutador é definido da seguinte forma

$$\{\hat{A}, \hat{B}\} = \hat{A}\hat{B} + \hat{B}\hat{A}. \tag{2.15}$$

Desde que essas relações são para operadores em geral, então elas podem ser aplicadas para quaisquer dois observáveis encontrados na literatura [24]. Por exemplo, como

$$[\hat{x}, \hat{p}_x] = i\hbar, \tag{2.16}$$

então

$$\Delta_x \Delta_{p_x} \geqslant \frac{\hbar}{2}. \tag{2.17}$$

2.1.3 Bits e Qbtis

A unidade de informação clássica é o bit. Um bit pode ter os valores lógicos "0" ou "1". Nos computadores, bits são fisicamente representados pela presença ou não de correntes elétricas em componentes eletrônicos dentro dos chips: a presença da corrente indica o estado lógico 1 e a sua ausência o estado lógico 0. Obviamente que os dois valores lógicos de um bit clássico são mutuamente excludentes.

Analogamente, a unidade de informação quântica é o bit quântico ou qbit. Um qbit pode ter os valores lógicos "0", "1" ou qualquer superposição deles. Fisicamente, qbits são representados por quaisquer objetos quânticos que possuam dois autoestados ortogonais. Os exemplos mais comuns são: estados de polarização de um fóton (horizontal ou vertical), elétrons em átomos de dois níveis (o que é uma aproximação), elétrons em poços quânticos, e *spins* nucleares [22].

Os estados de um qbit podem ser representados pelos seguintes kets

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \tag{2.18}$$

$$|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}. \tag{2.19}$$

O conjunto $\{|0\rangle, |1\rangle\}$ forma uma base no espaço de Hilbert de duas dimensões, chamada de base computacional. No caso de um *spin* 1/2 representa-se o qbit como sendo $|0\rangle \equiv |\uparrow\rangle$ e $|1\rangle \equiv |\downarrow\rangle$.

O estado genérico de um qbit é representado por

$$|\psi\rangle = a\,|0\rangle + b\,|1\rangle \tag{2.20}$$

em que $|a|^2 + |b|^2 = 1$. Esse estado pode ser parametrizado por ângulos θ e ϕ fazendo-se $a \equiv \cos(\theta/2)$ e $b \equiv \exp(i\phi)\,\mathrm{sen}(\theta/2)$

$$|\psi\rangle = \cos(\theta/2)\,|0\rangle + \exp(i\phi)\,\mathrm{sen}(\theta/2)\,|1\rangle\,. \tag{2.21}$$

Essa representação permite que o estado de um qbit seja visualizado como um ponto sobre a superfície de uma esfera. Tal esfera é chamada de esfera de Bloch.

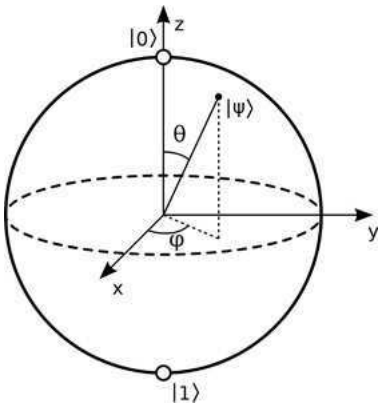

Figura 1 – Esfera de Bloch.

2.1.4 Vetores em Espaço Complexo Contínuo

O conjunto de vetores ortonormais e completos gerados por operadores lineares pode ser visto como um conjunto de vetores unitários ortogonais no espaço vetorial abstrato de Hilbert. A vantagem deste ponto de vista é que muitas propriedades matemáticas e manipulações envolvendo essas funções vêm analogamente de propriedades e operações que envolvem espaços vetoriais ordinários. Esses espaços são importantes quando o observável que se deseja medir tem espectro contínuo, tal como a posição e *momentum* de uma partícula [24].

Para ilustrar esse ponto de vista, seja $|\psi_1\rangle$ e $|\psi_2\rangle$ dois vetores, o seu produto interno é definido da seguinte forma

$$\langle\psi_1\,|\psi_2\rangle = \int \langle\psi_1\,|\alpha\rangle\langle\alpha\,|\psi_2\rangle\,d\alpha, \tag{2.22}$$

em que $\alpha = x + iy$, $x, y \in \Re$. Como exemplo, considere o caso da decomposição no estado $|p\rangle$, que representa o *momentum* de uma partícula, no espaço das posições, que é dada por

$$\langle x\,|p\rangle = \frac{1}{\sqrt{2\pi\hbar}} \exp\left(\frac{ipx}{\hbar}\right). \tag{2.23}$$

Isso impõe que a decomposição de uma estado qualquer $|\alpha\rangle$ no espaço dos momentos seja

$$\phi_\alpha(p) = \langle p\,|\alpha\rangle = \int dx \langle p\,|x\rangle\langle x\,|\alpha\rangle = \frac{1}{\sqrt{2\pi\hbar}} \int dx \exp\left(\frac{-ipx}{\hbar}\right)\psi_\alpha(x), \tag{2.24}$$

em que $\psi_\alpha(x) = \langle x\,|\alpha\rangle$ é a função de onda de $|\alpha\rangle$ no espaço das posições.

Pode-se notar que isto é uma generalização do produto interno para espaços complexos discretos, tais como aqueles que os qbits estão inseridos [24].

2.1.5 Aplicações dos Postulados

As matrizes de Pauli são importantes exemplos de transformações unitárias sobre 1 qbit:

$$\hat{X} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \tag{2.25}$$

$$\hat{Y} = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \tag{2.26}$$

$$\hat{Z} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}. \tag{2.27}$$

Uma outra operação unitária importante sobre 1 qbit é a transformação de Hadamard:

$$\hat{H} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} = \frac{X + Z}{\sqrt{2}}. \tag{2.28}$$

Considere agora o seguinte conjunto de operadores de medida de 1 qbit:

$$\hat{M}_0 \equiv |0\rangle\langle 0| \tag{2.29}$$

$$\hat{M}_1 \equiv |1\rangle\langle 1|\,. \tag{2.30}$$

Note que $\hat{M}_0$ e $\hat{M}_1$ são Hermitianos mas não são unitários. Isto quer dizer que o processo de medida representado por esses operadores é irreversível. Segundo o Postulado 3,

$$p_M(0) = \langle\psi| \hat{M}_0^\dagger \hat{M}_0 |\psi\rangle = |a|^2 \tag{2.31}$$

$$p_M(1) = \langle\psi| \hat{M}_1^\dagger \hat{M}_1 |\psi\rangle = |b|^2. \tag{2.32}$$

Após a medida,

$$|\psi_0\rangle = \frac{a}{|a|} |0\rangle \tag{2.33}$$

$$|\psi_1\rangle = \frac{b}{|b|} |1\rangle . \tag{2.34}$$

Os fatores $a/|a|$ e $b/|b|$ são fases globais (não observáveis), e podem ser descartados. Esses operadores de medidas são exemplos de projetores.

Os qbits de um espaço de Hilbert com dois qbits são obtidos pelo produto tensorial dos vetores do espaço de Hilbert com apenas um qbit

$$\{|0\rangle, |1\rangle\} \otimes \{|0\rangle, |1\rangle\} = \{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}. \tag{2.35}$$

A representação matricial de cada um desses vetores da base computacional de dois qbits é:

$$|00\rangle = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} \tag{2.36}$$

$$|01\rangle = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} \tag{2.37}$$

$$|10\rangle = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} \tag{2.38}$$

$$|11\rangle = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}. \tag{2.39}$$

A representação matricial das matrizes de Pauli e do operador de Hadamard nesta base pode ser obtida pelos produtos tensoriais correspondentes com a matriz identidade 2×2

$$\hat{O}_A = \hat{O} \otimes \hat{\mathcal{I}}, \tag{2.40}$$

$$\hat{O}_B = \hat{\mathcal{I}} \otimes \hat{O}, \tag{2.41}$$

em que $\hat{O} = \hat{X}, \hat{Y}, \hat{Z}, \hat{H}$. Aqui, adota-se a convenção $|AB\rangle$ para os estados do sistema composto. Essas expressões podem ser facilmente generalizadas para um número arbitrário de qbits [22].

2.1.6 Misturas Estatísticas e Matriz Densidade

Em Computação Quântica e Informação Quântica frequentemente é necessário lidar com situações em que o vetor de estado do sistema não é conhecido, mas apenas um conjunto possível de vetores ortonormais $|\psi_i\rangle$, que ocorrem com probabilidades $\{p_X(i)\}$ [24, 22]. O conjunto $\{p_X(i), |\psi_i\rangle\}$ é chamado de ensemble estatístico. A ferramenta matemática adequada para tratar esses casos é a matriz densidade, ρ, definida como

$$\rho \equiv \sum_i p_X(i) \, |\psi_i\rangle\langle\psi_i| \tag{2.42}$$

onde $p_X(i) \geqslant 0$ e $\sum_i p_X(i) = 1$. Algumas propriedades importantes deste operador:

1. A matriz densidade é um operador positivo, ou seja, possui autovalores reais não-negativos. De fato, para qualquer $|\phi\rangle$,

$$\langle\phi| \, \rho \, |\phi\rangle = \sum_i p_X(i) \langle\phi \, |\psi_i\rangle \, \langle\psi_i \, |\phi\rangle = \sum_i p_X(i) |\langle\phi \, |\psi_i\rangle|^2 > 0; \tag{2.43}$$

2. O traço de ρ é igual a 1:

$$Tr\{\rho\} = \sum_i p_X(i) Tr\{|\psi_i\rangle\langle\psi_i|\} = \sum_i p_X(i) = 1; \tag{2.44}$$

3. O estado será puro se e somente se $Tr(\rho^2) = 1$:

$$\rho^2 = \sum_i \sum_j p_X(i) p_X(j) \, |\psi_i\rangle\langle\psi_i \, |\psi_j\rangle\langle\psi_j| \tag{2.45}$$

$$= \sum_i p_X^2(i) \, |\psi_i\rangle\langle\psi_i| \, . \tag{2.46}$$

Consequentemente,

$$Tr\{\rho^2\} = \sum_i p_X^2(i) Tr\{|\psi_i\rangle\langle\psi_i|\} = \sum_i p_X^2(i) \leqslant 1 \tag{2.47}$$

A igualdade será satisfeita se e somente se $p_X(i) = 0$, exceto para um índice i_0 tal que $p_X(i_0) = 1$.

Qualquer operador positivo com traço igual a 1 é um operador densidade válido.

Os postulados da Mecânica Quântica podem ser reformulados em termos do operador densidade.

Quando se lida com sistemas compostos, dado o operador densidade do sistema total, os operadores densidade dos subsistemas podem ser obtidos através da operação de traço parcial. O traço parcial é uma soma sobre os estados de um dos subsistemas. Por exemplo, se ρ^{AB} for o operador densidade de um sistema composto AB, os operadores densidade de cada subsistema serão:

$$\rho^A \equiv Tr_B(\rho^{AB}) \tag{2.48}$$
$$\rho^B \equiv Tr_A(\rho^{AB}). \tag{2.49}$$

Estas relações são evidentes para sistemas não-emaranhados para os quais $\rho^{AB} = \rho^A \otimes \rho^B$.

2.2 Formalismo da Óptica Quântica

Será discutida a quantização do campo eletromagnético e suas propriedades básicas. Posteriormente, serão descritos alguns dos possíveis estados que a luz pode assumir. Em seguida, é dada uma explanação sobre os componentes comuns de estados quânticos em experimentos de óptica quântica.

2.2.1 Quantização do Campo Eletromagnético

A quantização do campo eletromagnético no espaço livre começa com a descrição clássica dada pelas equações de Maxwell [13, 26]. As equações de Maxwell criam uma ligação entre o campo elétrico $\mathbf{E}$ e o campo magnético $\mathbf{B}$ [27, 28]. No vácuo, onde não há cargas líquidas e nem correntes, as equações se tornam

$$\nabla \cdot \mathbf{E} = 0, \tag{2.50}$$
$$\nabla \cdot \mathbf{B} = 0, \tag{2.51}$$
$$\nabla \times \mathbf{E} + \frac{\partial \mathbf{B}}{\partial t} = 0, \tag{2.52}$$
$$\nabla \times \mathbf{B} - \mu_0 \epsilon_0 \frac{\partial \mathbf{E}}{\partial t} = 0. \tag{2.53}$$

Nessas equações, μ_0 e ϵ_0 são a permeabilidade magnética e a permissividade elétrica do vácuo, respectivamente. A velocidade da luz pode ser relacionada com essas quantidades pela seguinte relação

$$c = \frac{1}{\sqrt{\mu_0 \epsilon_0}}. \tag{2.54}$$

Pode ser mostrado que a dependência temporal e espacial do campo elétrico $\mathbf{E}(\mathbf{r}, t)$ é dada pela solução da equação

$$\Big(\nabla^2 - \frac{\partial^2}{\partial t^2}\Big)\mathbf{E} = 0. \tag{2.55}$$

A solução desta equação consiste em

$$\mathbf{E}(\mathbf{r}, t) = i \sum_{\mathbf{k}s} \Big(\frac{\hbar \omega_k}{2\epsilon_0 V}\Big)^{1/2} \mathbf{e}_{\mathbf{k}s} [\alpha_{\mathbf{k}s} u_{\mathbf{k}}(\mathbf{r}) e^{-i\omega_k t} - \alpha^*_{\mathbf{k}s} u^*_{\mathbf{k}}(\mathbf{r}) e^{i\omega_k t}], \tag{2.56}$$

em que $\hbar$ é a constante de Planck dividida por 2π, V é o volume de quantização do campo eletromagnético, $\mathbf{k}$ é o vetor de onda do modo, ω_k é a frequência angular do modo k, α e α^* são amplitudes complexas sem dimensão advindas da análise de Fourier e u é uma função do modo que descreve a sua polarização. A quantização do campo eletromagnético é feita pela troca de α e α^* pelos operadores de destruição e criação $\hat{a}$ e $\hat{a}^\dagger$, respectivamente. Usando o fato dos fótons serem bósons[4], a relação de comutação entre $\hat{a}$ e $\hat{a}^\dagger$ é

$$[\hat{a}_k, \hat{a}_k] = [\hat{a}^\dagger_k, \hat{a}^\dagger_k] = 0, \qquad [\hat{a}_k, \hat{a}^\dagger_k] = \delta_{kk}. \tag{2.57}$$

O campo quantizado assim se torna

$$\hat{\mathbf{E}}(\mathbf{r}, t) = i \sum_{\mathbf{k}s} \Big(\frac{\hbar \omega_k}{2\epsilon_0 V}\Big)^{1/2} \mathbf{e}_{\mathbf{k}s} [\hat{a}_{\mathbf{k}s} u_{\mathbf{k}}(\mathbf{r}) e^{-i\omega_k t} - \hat{a}^\dagger_{\mathbf{k}s} u^*_{\mathbf{k}}(\mathbf{r}) e^{i\omega_k t}], \tag{2.58}$$

O Hamiltoniano do campo será

$$\hat{\mathcal{H}} = \sum_k \hbar \omega_k \Big(\hat{a}^\dagger_k \hat{a}_k + \frac{1}{2}\Big). \tag{2.59}$$

Por fim, uma característica importante do espaço de Hilbert desse sistema é que ele é descrito pelos estados de Fock ou estados número $|n\rangle$. Eles representam o número de fótons, por exemplo, $|3\rangle$ é um sistema com três fótons. A ação dos operadores de destruição e criação sobre esses estados é

[4] Bósons são partículas que obedecem à estatística de Bose-Einstein [24]. Dentre os exemplos de bósons estão as partículas elementares, como o fóton, o glúon, o bóson de Higgs, e partículas compostas, como mésons e núcleos atômicos estáveis, como o hélio-4

$$\hat{a}\,|n\rangle = \sqrt{n}\,|n-1\rangle, \tag{2.60}$$

$$\hat{a}^{\dagger}\,|n\rangle = \sqrt{n+1}\,|n+1\rangle. \tag{2.61}$$

Com isso é possível entender o motivo do nome desses operadores.

2.2.2 Estados Quânticos da Luz de Interesse

Neste tópico será feita uma simplificação da teoria da óptica quântica desenvolvida anteriormente. Será adotado que o campo eletromagnético é monomodo. O motivo para isso é a simplicidade dos resultados obtidos.

2.2.2.1 Estado Térmico

Considere um campo eletromagnético monomodo em equilíbrio térmico dentro de uma cavidade de temperatura T. De acordo com a Mecânica Estatística [29], a probabilidade P_n de que o modo seja termicamente excitado para o n-ésimo nível de energia é

$$P_n = \frac{\exp(-E_n/k_BT)}{\sum_n \exp(-E_n/k_BT)} \tag{2.62}$$

em que E_n é a energia no n-ésimo nível e k_B é a constante de Boltzmann. O operador densidade para o campo térmico é dado por

$$\rho_{Th} = \frac{\exp(-\hat{\mathcal{H}}/k_BT)}{Tr\{\exp(-\hat{\mathcal{H}}/k_BT)\}} \tag{2.63}$$

em que $\hat{\mathcal{H}} = \hbar\omega(\hat{a}^{\dagger}\hat{a} + 1/2)$ e

$$Tr\{\exp(-\hat{\mathcal{H}}/k_BT)\} = \sum_{n=0}^{\infty} \langle n|\exp(-\hat{\mathcal{H}}/k_BT)\,|n\rangle \tag{2.64}$$

$$= \sum_{n=0}^{\infty} \exp(-E_n/k_BT) \equiv Z \tag{2.65}$$

é denominado função de partição. Com $E_n = \hbar\omega(n + 1/2)$

$$Z = \exp(-\hbar\omega/2k_BT) \sum_{n=0}^{\infty} \exp(-\hbar\omega n/k_BT). \tag{2.66}$$

Desde que $\exp(-\hbar\omega/k_BT) < 1$, então a soma é uma série geométrica e assim

$$\sum_{n=0}^{\infty} \exp(-\hbar\omega n/k_B T) = \frac{1}{1-\exp(-\hbar\omega/k_B T)} \tag{2.67}$$

de tal forma que

$$Z = \frac{\exp(-\hbar\omega/2k_B T)}{1-\exp(-\hbar\omega/k_B T)}. \tag{2.68}$$

Evidentemente

$$P_n = \langle n|\,\hat{\rho}_{Th}\,|n\rangle = \frac{1}{Z}\exp(-E_n/k_B T). \tag{2.69}$$

Também é possível notar que o operador densidade pode ser escrito como

$$\begin{aligned}
\rho_{Th} &= \sum_{n'=0}\sum_{n=0} |n'\rangle\langle n'|\,\rho_{Th}\,|n\rangle\langle n| && (2.70)\\
&= \frac{1}{Z}\sum_{n=0}^{\infty}\exp(-E_n/k_B T)\,|n\rangle\langle n| && (2.71)\\
&= \sum_{n=0}^{\infty} P_n\,|n\rangle\langle n|\,. && (2.72)
\end{aligned}$$

O número médio de fótons do campo térmico é calculado da seguinte forma

$$\begin{aligned}
\overline{n} &= \langle\hat{n}\rangle = Tr\{\hat{n}\hat{\rho}_{Th}\} = \sum_{n=0}^{\infty}\langle n|\,\hat{n}\rho_{Th}\,|n\rangle && (2.73)\\
&= \sum_{n=0}^{\infty} nP_n = \exp(-\hbar\omega/2k_B T)\frac{1}{Z}\sum_{n=0}^{\infty} n\exp(-\hbar\omega n/k_B T) && (2.74)\\
&= \frac{\exp(-\hbar\omega/k_B T)}{1-\exp(-\hbar\omega/k_B T)} && (2.75)\\
&= \frac{1}{\exp(\hbar\omega/k_B T)-1}. && (2.76)
\end{aligned}$$

Da Eq. (2.76) segue que

$$\exp(-\hbar\omega/k_B T) = \frac{\overline{n}}{1+\overline{n}} \tag{2.77}$$

e das Eqs. (2.69) e (2.72) segue que a matriz densidade ρ_{Th} pode ser escrita em termos de $\overline{n}$ como

$$\hat{\rho}_{Th} = \frac{1}{1+\overline{n}}\sum_{n=0}^{\infty}\left(\frac{\overline{n}}{1+\overline{n}}\right)^n |n\rangle\langle n|\,. \tag{2.78}$$

A probabilidade de encontrar n fótons em um campo térmico em, termos de $\overline{n}$, é

$$P_n = \frac{\overline{n}^n}{(1+\overline{n})^{n+1}}. \tag{2.79}$$

A variância do número de fótons é dada por

$$\Delta_n^2 = \langle \hat{n}^2 \rangle - \langle \hat{n} \rangle^2. \tag{2.80}$$

Como

$$\begin{aligned} \langle \hat{n}^2 \rangle &= Tr(\overline{n}^2 \hat{\rho}_{Th}) && (2.81)\\ &= \overline{n} + 2\overline{n}^2, && (2.82) \end{aligned}$$

então

$$\Delta_n^2 = \overline{n} + \overline{n}^2, \tag{2.83}$$

o que mostra que a variância é consideravelmente maior do que sua média.

Como é mostrado no livro de Knight [26], a energia média por unidade de volume para o estado térmico é obtida como sendo

$$\overline{U} = \frac{\pi^2 k_B^4 T^4}{15 c^3 \hbar^3}, \tag{2.84}$$

em que T é a temperatura e c é a velocidade da luz. Essa expressão da Eq. (2.84) é conhecida como lei de Stefan-Boltzmann.

2.2.2.2 Estados Coerentes

Para os estados número $|n\rangle$, tem-se que o valor do campo elétrico é zero, $\langle n| \hat{\mathbf{E}} |n\rangle = 0$, o que não condiz com a maioria das realizações físicas de experimentos. Os estados que mais se aproximam dos estados clássicos e que não possuem essa característica de campo elétrico nulo são os estados coerentes. Estes estados são denotados por $|\alpha\rangle$ e são os autoestados do operador $\hat{a}$,

$$\hat{a} |\alpha\rangle = \alpha |\alpha\rangle, \tag{2.85}$$

em que α é um número complexo.

Desde que os estados números $|n\rangle$ formam um conjunto completo, então pode-se expandir $|\alpha\rangle$ de acordo com

$$|\alpha\rangle = \sum_{n=0}^{\infty} C_n |n\rangle . \tag{2.86}$$

Aplicando $\hat{a}$ na Eq. (2.86) e lembrando que o resultado é novamente $|\alpha\rangle$, pela Eq. (2.85), tem-se que[5]

$$\hat{a}|\alpha\rangle = \sum_{n=1}^{\infty} C_n \sqrt{n} |n-1\rangle = \alpha \sum_{n=0}^{\infty} C_n |n\rangle . \tag{2.87}$$

Igualando os coeficientes de $|n\rangle$

$$C_n \sqrt{n} = \alpha C_{n-1} \tag{2.88}$$

ou

$$C_n = \frac{\alpha}{\sqrt{n}} C_{n-1} = \frac{\alpha^2}{\sqrt{n(n-1)}} C_{n-2} = \cdots \tag{2.89}$$

$$= \frac{\alpha^n}{\sqrt{n!}} C_0 \tag{2.90}$$

e assim,

$$|\alpha\rangle = C_0 \sum_{n=0}^{\infty} \frac{\alpha^n}{\sqrt{n!}} |n\rangle . \tag{2.91}$$

Pelo critério de normalização se determina C_0

$$\langle \alpha | \alpha \rangle = 1 = |C_0|^2 \sum_n \sum_{n'} \frac{{\alpha^*}^n \alpha^{n'}}{\sqrt{n! n'!}} \langle n | n' \rangle \tag{2.92}$$

$$= |C_0|^2 \sum_{n=0}^{\infty} \frac{|\alpha|^{2n}}{n!} = |C_0|^2 e^{|\alpha|^2}, \tag{2.93}$$

no qual implica que $C_0 = \exp(-\frac{1}{2}|\alpha|^2)$. Assim, o estado coerente normalizado é igual a

$$|\alpha\rangle = \exp(-\frac{1}{2}|\alpha|^2) \sum_{n=0}^{\infty} \frac{\alpha^n}{\sqrt{n!}} |n\rangle . \tag{2.94}$$

Será feita uma análise do valor médio do operador campo elétrico que tem componente em x

[5] Usamos a álgebra correspondente às relações das Eqs. (2.57) e (2.61).

$$\hat{E}_x(\vec{r},t) = i\Big(\frac{\hbar\omega}{2\epsilon_0 V}\Big)^{1/2}\left[\hat{a}e^{i(\vec{k}\cdot\vec{r}-\omega t)} - \hat{a}^\dagger e^{-i(\vec{k}\cdot\vec{r}-\omega t)}\right]. \tag{2.95}$$

Para ele é obtido que

$$\begin{aligned}\langle\alpha|\,\hat{E}_x\,|\alpha\rangle &= i\Big(\frac{\hbar\omega}{2\epsilon_0 V}\Big)^{1/2}\left[\alpha e^{i(\vec{k}\cdot\vec{r}-\omega t)} - \alpha^* e^{-i(\vec{k}\cdot\vec{r}-\omega t)}\right] &(2.96)\\ &= 2|\alpha|\Big(\frac{\hbar\omega}{2\epsilon_0 V}\Big)^{1/2}\operatorname{sen}(\omega t - \vec{k}\cdot\vec{r} - \theta), &(2.97)\end{aligned}$$

em que $\alpha = |\alpha|e^{i\theta}$ e no qual tem as características do campo elétrico de uma onda propagante. Para o cálculo da variância do campo, é necessário que se tenha o segundo momento do campo

$$\langle\alpha|\,\hat{E}_x^2\,|\alpha\rangle = \frac{\hbar\omega}{2\epsilon_0 V}\left[1 + 4|\alpha|^2\operatorname{sen}^2(\omega t - \vec{k}\cdot\vec{r} - \theta)\right]. \tag{2.98}$$

Assim, a flutuação ou variância de $\hat{E}_x$ é

$$\Delta E_x \equiv \langle(\Delta\hat{E}_x)^2\rangle^{1/2} = \Big(\frac{\hbar\omega}{2\epsilon_0 V}\Big)^{1/2}, \tag{2.99}$$

o que é idêntico à variância do estado do vácuo. O estado coerente é o mais clássico por que não apenas tem a forma correta para o valor médio do campo elétrico mas também contém o ruído caracterizado como apenas o ruído do vácuo.

A seguir, apresenta-se uma interpretação física da variável α na expressão do estado coerente. O valor esperado do operador número de fótons para o estado coerente é

$$\overline{n} = \langle\alpha|\,\hat{n}\,|\alpha\rangle = |\alpha|^2 \tag{2.100}$$

assim, $|\alpha|^2$ é apenas o número médio de fótons no campo. O segundo momento do número de fótons é dado por

$$\begin{aligned}\langle\alpha|\,\hat{n}^2\,|\alpha\rangle &= \langle\alpha|\,\hat{a}^\dagger\hat{a}\hat{a}^\dagger\hat{a}\,|\alpha\rangle &(2.101)\\ &= \langle\alpha|\,(\hat{a}^\dagger\hat{a}^\dagger\hat{a}\hat{a} + \hat{a}^\dagger\hat{a})\,|\alpha\rangle &(2.102)\\ &= |\alpha|^4 + |\alpha|^2 = \overline{n}^2 + \overline{n} &(2.103)\end{aligned}$$

e assim

$$\Delta n = \sqrt{\langle\hat{n}^2\rangle - \langle\hat{n}\rangle^2} = \overline{n}^{1/2}, \tag{2.104}$$

no qual tem característica de processo de Poisson. De fato, para uma medida do número de fótons no campo, a probabilidade de detectar n fótons é

$$P_n = |\langle n\,|\alpha\rangle\,|^2 = e^{-|\alpha|^2}\frac{|\alpha|^{2n}}{n!} \tag{2.105}$$

$$= e^{-\overline{n}}\frac{\overline{n}^n}{n!}, \tag{2.106}$$

no qual é uma distribuição de Poisson com média $\overline{n}$. Note que a indeterminação com relação ao valor médio de fótons é

$$\frac{\Delta n}{\overline{n}} = \frac{1}{\sqrt{\overline{n}}}, \tag{2.107}$$

no qual diminui com o aumento de $\overline{n}$.

Os estados coerentes $|\alpha\rangle$ são os estados quânticos mais próximos dos estados clássicos pois: (i) o valor esperado do campo elétrico tem a forma da expressão clássica; (ii) a flutuação no campo elétrico é a mesma para o vácuo; (iii) a flutuação do número médio de fótons com relação ao valor médio decresce com o aumento do número médio de fótons.

Será discutida agora uma forma de se obter os estados coerentes por meio da aplicação do operador de deslocamento no estado do vácuo.

O operador de deslocamento é definido como sendo

$$\hat{D}(\alpha) = \exp(\alpha\hat{a}^\dagger - \alpha^*\hat{a}) \tag{2.108}$$

e os estados coerentes são dados por

$$|\alpha\rangle = \hat{D}(\alpha)\,|0\rangle\,. \tag{2.109}$$

Esse resultado é obtido da identidade

$$e^{\hat{A}+\hat{B}} = e^{\hat{A}}e^{\hat{B}}e^{-\frac{1}{2}\left[\hat{A},\hat{B}\right]} \tag{2.110}$$

$$= e^{\hat{B}}e^{\hat{A}}e^{\frac{1}{2}\left[\hat{B},\hat{A}\right]} \tag{2.111}$$

no qual é válida se $\left[\hat{A},\hat{B}\right] \neq 0$ e $\left[\hat{A},\left[\hat{A},\hat{B}\right]\right] = \left[\hat{B},\left[\hat{A},\hat{B}\right]\right] = 0$. Com $\hat{A} = \alpha\hat{a}^\dagger$ e $\hat{B} = -\alpha^*\hat{a}$, $\left[\hat{A},\hat{B}\right] = |\alpha|^2$, tem-se que a Eq. (2.108) resulta em

$$\hat{D}(\alpha) = e^{\alpha\hat{a}^\dagger - \alpha^*\hat{a}} = e^{-\frac{1}{2}|\alpha|^2}e^{\alpha\hat{a}^\dagger}e^{-\alpha^*\hat{a}}. \tag{2.112}$$

Expandindo $\exp(-\alpha^*\hat{a})$ em séries de Taylor, tem-se que

$$e^{-\alpha^*\hat{a}}\,|0\rangle = \sum_{l=0}^{\infty} \frac{(-\alpha^*\hat{a})^l}{l!}\,|0\rangle = |0\rangle\,. \tag{2.113}$$

Mas como

$$\begin{aligned} e^{\alpha\hat{a}^\dagger}\,|0\rangle &= \sum_{n=0}^{\infty} \frac{(\alpha\hat{a})^n}{n!}\,|0\rangle & (2.114)\\ &= \sum_{n=0}^{\infty} \frac{\alpha^n}{\sqrt{n!}}\,|n\rangle\,, & (2.115)\end{aligned}$$

então

$$\begin{aligned} |\alpha\rangle &= \hat{D}(\alpha)\,|0\rangle & (2.116)\\ &= e^{-\frac{1}{2}|\alpha|^2} \sum_{n=0}^{\infty} \frac{\alpha^n}{\sqrt{n!}}\,|n\rangle\,, & (2.117)\end{aligned}$$

o que está de acordo com a definição de estados coerentes.

O operador deslocamento é um operador unitário. Por isso,

$$\begin{aligned} \hat{D}^\dagger(\alpha) &= \hat{D}(-\alpha) & (2.118)\\ &= e^{-\frac{1}{2}|\alpha|^2} e^{-\alpha\hat{a}^\dagger} e^{\alpha^*\hat{a}}. & (2.119)\end{aligned}$$

É evidente que $\hat{D}(\alpha)\hat{D}^\dagger(\alpha) = \hat{D}^\dagger(\alpha)\hat{D}(\alpha) = \mathcal{I}$.

O operador deslocamento obedece à relação de semigrupo: o produto de dois operadores deslocamento, por exemplo $\hat{D}(\alpha)$ e $\hat{D}(\beta)$, é, a menos de um fator de fase global, o operador deslocamento $\hat{D}(\alpha+\beta)$. Para obter esse resultado, tem-se que notar que se for feita a consideração que se $\hat{A} = \alpha\hat{a}^\dagger - \alpha^*\hat{a}$ e $\hat{B} = \beta\hat{a}^\dagger - \beta^*\hat{a}$, então

$$\left[\hat{A}, \hat{B}\right] = \alpha\beta^* - \alpha^*\beta = 2i\Im m(\alpha\beta^*). \tag{2.120}$$

Assim, usando a Eq. 2.111 é possível obter que

$$\begin{aligned} \hat{D}(\alpha)\hat{D}(\beta) &= e^{\hat{A}} e^{\hat{B}} & (2.121)\\ &= \exp\left[i\Im m(\alpha\beta^*)\right] e^{(\alpha+\beta)\hat{a}^\dagger - (\alpha^*+\beta^*)\hat{a}^\dagger} & (2.122)\\ &= \exp\left[i\Im m(\alpha\beta^*)\right] \hat{D}(\alpha+\beta). & (2.123)\end{aligned}$$

Isso resulta que a aplicação deste produto de operadores deslocamento sobre o estado do vácuo resulta em

$$\hat{D}(\alpha)\hat{D}(\beta)\left|0\right\rangle = \hat{D}(\alpha)\left|\beta\right\rangle \tag{2.124}$$

$$= \exp\left[i\Im m(\alpha\beta^*)\right]\left|\alpha+\beta\right\rangle, \tag{2.125}$$

em que a fase global $\exp\left[i\Im m(\alpha\beta^*)\right]$ não tem interesse físico relevante[22].

Se for considerado que o operador vetorial, que representa a posição e o *momentum*, seja dado por $\hat{\mathbf{R}} = (q_1, p_1)$, então ação do operador de deslocamento sobre esse vetor será [30]

$$D^\dagger(\alpha)\hat{\mathbf{R}}D(\alpha) = (q_1 + \Re e\{\alpha\}, p_1 + \Im m\{\alpha\}). \tag{2.126}$$

Como a variância dessa quantidade é a mesma do vácuo, então a matriz de covariância será

$$\mathbf{\Sigma}_\alpha = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}. \tag{2.127}$$

2.2.2.3 Estados Comprimidos

Será apresentado o exemplo mais importante de estados da luz não-clássicos. Os estados comprimidos serão caracterizados pelos mesmos aspectos que foram relevantes para os estados coerentes, estatística de fóton, produção dos mesmos pelo estado do vácuo, entre outros.

Primeiramente, considere dois operadores $\hat{A}$ e $\hat{B}$ satisfazendo a relação de comutação $\left[\hat{A}, \hat{B}\right] = i\hat{C}$, o que resulta que

$$\langle(\Delta\hat{A})^2\rangle\langle(\Delta\hat{B})^2\rangle \geqslant \frac{1}{4}|\langle\hat{C}\rangle|^2. \tag{2.128}$$

Um estado do sistema é dito ser comprimido se ou

$$\langle(\Delta\hat{A})^2\rangle < \frac{1}{2}|\langle\hat{C}\rangle| \tag{2.129}$$

ou

$$\langle(\Delta\hat{B})^2\rangle < \frac{1}{2}|\langle\hat{C}\rangle|. \tag{2.130}$$

No caso de estados comprimidos que serão mostrados neste trabalho, tem-se que $\hat{A} = \hat{X}_1$ e $\hat{B} = \hat{X}_2$, com $\hat{X}_1$ e $\hat{X}_2$ sendo os operadores de quadratura do campo.

Esses estados, para os quais uma das componentes obedece à condição de compressão, têm a característica que esta componente terá ruído, ou variância, menor do que a do estado coerente ou do vácuo. Porém, a outra componente terá uma flutuação maior, com relação a do vácuo, para que a relação de indeterminação seja satisfeita.

Uma maneira de se obter os estados comprimidos é por meio do operador de *squeeze* (ou compressão), que será chamado de operador de compressão, que é definido como sendo

$$\hat{S}(\xi) = \exp\left[\frac{1}{2}(\xi^* \hat{a}^2 - \xi \hat{a}^{\dagger 2})\right], \tag{2.131}$$

em que $\xi = re^{i\theta}$, para $0 \leqslant r < \infty$ e $0 \leqslant \theta \leqslant 2\pi$. O parâmetro r é conhecido como parâmetro (ou fator) de compressão.

Esse operador $\hat{S}(\xi)$ é tipo uma generalização do operador de deslocamento para dois fótons. Assim, a ação de $\hat{S}(\xi)$ sobre o vácuo criará algum tipo de estado coerente de dois fótons.

Para entender o que acontece quando se aplica esse operador, considere

$$|\psi_s\rangle = \hat{S}(\xi)\,|\psi\rangle \tag{2.132}$$

em que $|\psi\rangle$ é, por enquanto, arbitrário e $|\psi_s\rangle$ denota o estado gerado pela ação de $\hat{S}(\xi)$ sobre $|\psi\rangle$. Para obter as variâncias de $\hat{X}_1$ e $\hat{X}_2$, são necessários os valores esperados de $\hat{a}$, $\hat{a}^2$, etc. Para isso, é usado o seguinte resultado obtido da aplicação do lema de Baker-Hausdorff [26]

$$\hat{S}^\dagger(\xi)\hat{a}\hat{S}(\xi) = \hat{a}\cosh r - \hat{a}^\dagger e^{i\theta}\sinh r \tag{2.133}$$

$$\hat{S}^\dagger(\xi)\hat{a}^\dagger\hat{S}(\xi) = \hat{a}^\dagger\cosh r - \hat{a}e^{-i\theta}senhr, \tag{2.134}$$

em que $\hat{S}^\dagger(\xi) = \hat{S}(-\xi)$. Assim,

$$\langle\psi_s|\,\hat{a}\,|\psi_s\rangle = \langle\psi|\,\hat{S}^\dagger(\xi)\hat{a}\hat{S}(\xi)\,|\psi\rangle \tag{2.135}$$

e

$$\langle\psi_s|\,\hat{a}^2\,|\psi_s\rangle = \langle\psi|\,\hat{S}^\dagger(\xi)\hat{a}\hat{S}(\xi)\hat{S}^\dagger(\xi)\hat{a}\hat{S}(\xi)\,|\psi\rangle\,, \tag{2.136}$$

etc. Para o caso especial onde $|\psi\rangle$ é o estado do vácuo $|0\rangle$, $|\psi_s\rangle$ é o estado comprimido do vácuo, no qual é denotado por $|\xi\rangle$

$$|\xi\rangle = \hat{S}(\xi)\,|0\rangle\,. \tag{2.137}$$

Usando as Eqs. (2.134-2.137) é obtido que

$$\langle(\Delta\hat{X}_1)^2\rangle = \frac{1}{4}\left[\cosh^2 r + \sinh^2 r - 2\sinh r\cosh r\cos\theta\right], \tag{2.138}$$

$$\langle(\Delta\hat{X}_2)^2\rangle = \frac{1}{4}\left[\cosh^2 r + \sinh^2 r + 2\sinh r\cosh r\cos\theta\right]. \tag{2.139}$$

Para $\theta = 0$

$$\langle(\Delta\hat{X}_1)^2\rangle = \frac{1}{4}e^{-2r}, \tag{2.140}$$

$$\langle(\Delta\hat{X}_2)^2\rangle = \frac{1}{4}e^{2r}. \tag{2.141}$$

e é possível notar que existe uma compressão na quadratura $\hat{X}_1$ dependentes de r. Para $\theta = \pi$, a compressão ocorrerá na quadratura $\hat{X}_2$.

Um estado comprimido mais geral pode ser obtido com o auxílio do operador deslocamento

$$|\alpha,\xi\rangle = \hat{D}(\alpha)\hat{S}(\xi)\,|0\rangle\,. \tag{2.142}$$

Para $\xi = 0$ se obtém um estado coerente. Desde que se tem

$$\hat{D}^\dagger\hat{a}\hat{D}(\alpha) = \hat{a} + \alpha \tag{2.143}$$

$$\hat{D}^\dagger\hat{a}^\dagger\hat{D}(\alpha) = \hat{a}^\dagger + \alpha^*, \tag{2.144}$$

então a ação do produto dos operadores deslocamento e compressão sobre $\hat{a}$ e $\hat{a}^\dagger$ pode ser obtida das Eqs. (2.134) e (2.144). Com as informações anteriores, é possível mostrar que

$$\langle\hat{a}\rangle = \alpha, \tag{2.145}$$

no qual é independente do parâmetro de compressão r, e

$$\langle \hat{a}^2 \rangle = \alpha^2 - e^{i\theta} \sinh r \cosh r, \tag{2.146}$$

$$\langle \hat{a}^\dagger \hat{a} \rangle = |\alpha|^2 + senh^2 r. \tag{2.147}$$

As propriedades do estado coerente são obtidas fazendo $r = 0$ e o estado do vácuo comprimido para $\alpha = 0$.

Para se ter uma ideia melhor dos estados comprimidos e a expressão deles em termo dos estados número, deve-se primeiramente observar que

$$\hat{a} \, |0\rangle = 0. \tag{2.148}$$

Multiplicando o lado esquerdo por $\hat{S}(\xi)$ e adicionando o operador unitário é possível ver que

$$\hat{S}(\xi)\hat{a}\hat{S}^\dagger(\xi)\hat{S}(\xi) \, |0\rangle = 0 \tag{2.149}$$

ou

$$\hat{S}(\xi)\hat{a}\hat{S}^\dagger(\xi) \, |\xi\rangle = 0. \tag{2.150}$$

Desde que

$$\hat{S}(\xi)\hat{a}\hat{S}^\dagger(\xi) = \hat{a} \cosh r + e^{i\theta}\hat{a}^\dagger \sinh r, \tag{2.151}$$

então, pode-se escrever a Eq. (2.150) como

$$(\hat{a}\mu + \hat{a}^\dagger \nu) \, |\xi\rangle = 0, \tag{2.152}$$

em que $\mu = \cosh r$ e $\nu = e^{i\theta} \sinh r$. Assim, o estado do vácuo comprimido é um autoestado do operador $\hat{a}\mu + \hat{a}^\dagger\nu$ com autovalor zero. Para o caso mais geral, considere o estado da Eq. (2.142), no qual é possível escrever que

$$\hat{D}(\alpha)\hat{S}(\xi)\hat{a}\hat{S}^\dagger(\xi)\hat{D}^\dagger(\alpha)\hat{D}(\alpha)\hat{S}(\xi) \, |0\rangle = 0, \tag{2.153}$$

usando a relação

$$\hat{D}(\alpha)\hat{a}\hat{D}^{\dagger}(\alpha)(\alpha) = \hat{a} - \alpha. \tag{2.154}$$

Assim, a Eq. (2.152) pode ser reescrita como

$$(\hat{a}\mu + \hat{a}^{\dagger}\nu)\,|\alpha,\xi\rangle = \gamma\,|\alpha,\xi\rangle\,, \tag{2.155}$$

em que $\gamma = \alpha\cosh r + \alpha^{*}e^{i\theta}\sinh r$. Para $r = 0$, tem-se o problema de autovalor do estado coerente e $\alpha = 0$ como sendo o problema de autovalor do estado do vácuo comprimido.

Se for feita a decomposição dos estados comprimidos nos estados número, tem-se que

$$|\xi\rangle = \sum_{n=0}^{\infty} C_n\,|n\rangle, \tag{2.156}$$

fazendo-se a substituição da Eq. (2.156) na Eq. (2.152), obtêm-se

$$C_{n+1} = -\frac{\nu}{\mu}\Big(\frac{n}{n+1}\Big)^{1/2} C_{n-1}. \tag{2.157}$$

Note que esta solução envolve duas partes, uma para os estados número ímpares e outra para os pares. Observa-se que apenas a solução par contém o estado do vácuo. Para esta solução par, tem-se que

$$C_{2m} = (-1)^m (e^{i\theta}\tanh r)^m \left[\frac{(2m-1)!!}{(2m)!!}\right]^{1/2} C_0. \tag{2.158}$$

Em que $n!!$ representa o duplo fatorial do inteiro n, ou seja, $n!! = (n!)!$, e C_0 é determinado pela condição de normalização

$$\sum_{m=0}^{\infty} |C_{2m}|^2 = 1, \tag{2.159}$$

no qual leva a

$$|C_0|^2(1 + \sum_{m=0}^{\infty} \frac{(\tanh r)^{2m}(2m-1)!!}{(2m)!!}) = 1. \tag{2.160}$$

Como existe uma identidade que diz que

$$1 + \sum_{m=0}^{\infty} z^m(\frac{(2m-1)!!}{(2m)!!}) = (1-z)^{-1/2}, \tag{2.161}$$

então é obtido $C_0 = \sqrt{\cosh r}$. Finalmente, pela identidade

$$(2m)!! = 2^m m! \tag{2.162}$$

$$(2m-1)!! = \frac{1}{2^m}\frac{(2m)!}{m!}, \tag{2.163}$$

então

$$C_{2m} = (-1)^m \frac{\sqrt{(2m)!}}{2^m m!}\frac{(e^{i\theta}\tanh r)^m}{\sqrt{\cosh r}}. \tag{2.164}$$

Assim, o estado do vácuo comprimido é

$$|\xi\rangle = \frac{1}{\sqrt{\cosh r}}\sum_{m=0}^{\infty}(-1)^m \frac{\sqrt{(2m)!}}{2^m m!}e^{im\theta}(\tanh r)^m |2m\rangle . \tag{2.165}$$

A probabilidade de se detectar $2m$ fótons no campo é

$$P_{2m} = |\langle 2m|\xi\rangle| = \frac{(2m)!}{2^{2m}(m!)^2}\frac{(\tanh r)^{2m}}{\cosh r}, \tag{2.166}$$

enquanto que a probabilidade de detectar $2m+1$ é

$$P_{2m+1} = |\langle 2m+1|\xi\rangle| = 0. \tag{2.167}$$

Assim, a distribuição de probabilidade do estado comprimido do vácuo é oscilatória, desaparecendo para os números de fótons ímpares.

É mostrado na Ref. [26] que a solução para a Eq. 2.155 é

$$\begin{aligned}|\alpha,\epsilon\rangle = \quad & \tfrac{1}{\sqrt{\cosh r}}\exp\left[-\tfrac{1}{2}|\alpha|^2 - \tfrac{1}{2}\alpha^{*2}e^{i\theta}\tanh r\right]\times \\ & \textstyle\sum_{n=0}^{\infty}\frac{\left[\frac{1}{2}e^{i\theta}\tanh r\right]^{n/2}}{\sqrt{n!}}H_n\left[\gamma(e^{i\theta}\sinh(2r))^{-1/2}\right]|n\rangle ,\end{aligned} \tag{2.168}$$

em que H_n são os polinômios de Hermite. A probabilidade de se encontrar n fótons no campo é dada por

$$P_n = |\langle n|\alpha,\xi\rangle|^2 \tag{2.169}$$

$$\begin{aligned} = \quad & \tfrac{(\frac{1}{2}\tanh r)^n}{n!\cosh r}\exp\left[-|\alpha|^2 - \tfrac{1}{2}(\alpha^{*2}e^{i\theta} + \alpha^2 e^{-i\theta})\tanh r\right]\times \\ & |H_n\left[\gamma(e^{i\theta}\sinh(2r))^{-1/2}\right]|^2. \end{aligned} \tag{2.170}$$

Se $|\alpha|^2 \gg \sinh^2 r$, é dito que a parte "coerente" do estado domina a parte comprimida. Da Eq. (2.170) é evidende que a distribuição depende da fase α.

De forma similar como foi feito em 2.126, mas com a observação que para o estado comprimido é o deslocamento, com relação à origem é feito pela aplicação do operador de deslocamento, então tem-se que a matriz $\mathbf{R}$ será a mesma de 2.126, mas a matriz de covariância mudará. Seja σ antes da aplicação do operador de compressão, com isso, essa matriz evoluirá para a matriz

$$\sigma \rightarrow \mathbf{\Sigma}_{\xi}\sigma\mathbf{\Sigma}_{\xi}, \tag{2.171}$$

em que

$$\mathbf{\Sigma}_{\xi} = \begin{pmatrix} \mu + \Re e\{\nu\} & \Im m\{\nu\} \\ \Im m\{\nu\} & \mu - \Re e\{\nu\} \end{pmatrix} \tag{2.172}$$

2.2.2.4 Estado Comprimido Bimodal Usado no Protocolo

A compressão sobre um estado bimodal é descrito pelo Hamiltoniano $\hat{\mathcal{H}} \propto \hat{a}^{\dagger}\hat{b}^{\dagger} + \hat{a}\hat{b}$, com $\hat{a}$ e $\hat{b}$ sendo os operadores de destruição do modo 1 e 2, respectivamente. O operador de compressão é dado por

$$\hat{S}_2(\xi) = \exp(\xi\hat{a}^{\dagger}\hat{b}^{\dagger} - \xi^{*}\hat{a}\hat{b}), \tag{2.173}$$

em que $\xi = re^{i\psi}$. Como no caso monomodo, tem-se que $\mu = coshr$ e $\nu = e^{i\psi}sinhr$. A ação desse operador sobre o estado do vácuo pode ser descrita pela equação

$$\hat{S}_2(\xi)\left|0\right\rangle\left|0\right\rangle = \frac{1}{\sqrt{\mu}}\sum_{k=0}^{\infty}\left(\frac{\nu}{\mu}\right)^{k}\left|k\right\rangle\left|k\right\rangle \tag{2.174}$$

e é conhecido como estado do vácuo bimodal comprimido [31].

Uma quantidade bastante importante, principalmente para justificar a viabilidade do protocolo de QKD que será proposto posteriormente, é a matriz de covariância do estado comprimido bimodal. Se for considerado que a matriz de covariância do estado antes de sofrer a ação do operador de compressão seja igual a σ, então o operador de compressão fará com que ela evolua para

$$\sigma \rightarrow \mathbf{\Sigma}_{2\xi}\sigma\mathbf{\Sigma}_{2\xi}^{T}, \tag{2.175}$$

em que

$$\mathbf{\Sigma}_{2\xi} = \begin{pmatrix} \mu & 0 & \Re e\{\nu\} & \Im m\{\nu\} \\ 0 & \mu & \Im m\{\nu\} & -\Re e\{\nu\} \\ \Re e\{\nu\} & \Im m\{\nu\} & \mu & 0 \\ \Im m\{\nu\} & -\Re e\{\nu\} & 0 & \mu \end{pmatrix}. \tag{2.176}$$

Uma característica importante de uma matriz covariância é que ela fornece a direção e a magnitude da compressão que é feita sobre o estado. O autovetor dessa matriz corresponde às direções em que está sendo feita a compressão, ou o alargamento, e o autovalor respectivo diz à sua magnitude [32].

Será apresentado a seguir, Capítulo 3, os motivos pelos quais houve a necessidade de se construir a criptografia quântica. Dois dos principais protocolos são apresentados, o BB84 e o desenvolvido por Cerf [33], em 2001. Além disso, mesmo não sendo utilizado nesse trabalho, a parte da criptografia quântica que é tratada classicamente, a parte da reconciliação e a de amplificação de privacidade, também será explanada.

3 Criptografia Clássica e Quântica

O alto tráfego de informação devido ao aparecimento de novas tecnologias de comunicação e a sensibilidade quanto aos dados trafegados têm feito da criptografia uma necessidade cada vez mais importante em diversas aplicações. Este capítulo tem como objetivo introduzir os principais conceitos desse campo que serão utilizados para o desenvolvimento deste trabalho.

3.1 Introdução à Criptografia Clássica

A criptologia pode ser dividida em duas áreas principais; a criptografia e a criptoanálise [2]. A primeira abrange todo o esforço de se estabelecer uma transmissão segura da informação viabilizando diferentes características, como confidencialidade, integridade de dados, autenticação e irretratabilidade. Já a criptoanálise reúne todas as técnicas que tem como objetivo obter, de forma não autorizada, mensagens geradas por algum processo de criptografia.

Frequentemente utilizado na literatura sobre criptografia [2, 1, 3], o conceito de transmissão segura de informação, utilizando métodos criptográficos, possui três personagens principais para ilustrar seu funcionamento: Alice, Bob e Eva. Como padrão, Alice deseja enviar uma mensagem de forma segura a Bob, ou seja, prevenindo que Eva (a espiã) acesse a informação original e, além disso, que Eva seja capaz de enviar mensagens a Bob se passando por Alice.

Para isso, Alice realiza o processo de cifragem da mensagem original, frequentemente referenciada como mensagem simples, produzindo uma mensagem secreta tal que

$$C = \mathrm{Enc}\{M\}, \tag{3.1}$$

em que M representa a mensagem simples, $\mathrm{Enc}\{\cdot\}$ a função de encriptação de Alice e C a mensagem cifrada. Dessa forma, o processo de cifragem está relacionado à codificação da mensagem, enquanto o oposto, a decifragem, se relaciona à decodificação. Bob recebe então C, a partir de um canal de comunicação, e, por meio da aplicação de uma função de decifragem correspondendo a $\mathrm{Dec}\{\cdot\}$, obtém a mensagem original, ou seja,

$$M = \mathrm{Dec}\{C\}. \tag{3.2}$$

A segurança da transmissão da informação, nesse caso, é mantida pelas funções $\mathrm{Enc}\{\cdot\}$ e $\mathrm{Dec}\{\cdot\}$, que devem ser mantidas em segredo. Entretanto, essa abordagem não é

prática o suficiente, pois requer uma grande quantidade de diferentes funções, sendo duas funções para cada um dos usuários que Alice se comunique, o que é bastante alto em um sistema de comunicação real. Além disso, implementações de *hardware*, ou *software*, de diversas funções distintas é um processo conhecidamente ineficiente[1].

Uma forma de contornar esse problema é, ao invés de manter a função como elemento secreto, utilizar um argumento para uma dada função conhecida por ambos os pares da comunicação[1] e utilizar então esse argumento como a informação secreta compartilhada. Esse argumento secreto é referenciado como chave criptográfica e faz com que as Eqs. (3.1) e (3.2) se tornem

$$C = \mathrm{Enc}_k\{M\}, \tag{3.3}$$

$$M = \mathrm{Dec}_k\{C\}, \tag{3.4}$$

em que as funções $\mathrm{Enc}\{\cdot\}$ e $\mathrm{Dec}\{\cdot\}$ dependem agora de outro argumento, que é a chave criptográfica k. A Fig. 2 apresenta um diagrama que resume as operações definidas.

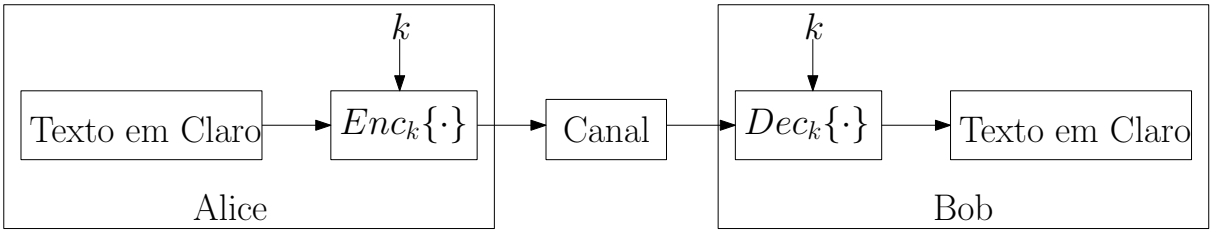

Figura 2 – Sistema criptográfico simples para transmissão segura da informação.

É possível criar métodos de criptografia que utilizem chaves diferentes nos processos de cifragem e decifragem, que é o método de criptografia de chave assimétrica, mas o conhecimento desses não será necessário neste trabalho. A seguir será apresentada a criptografia de chave simétrica, que é a base pelo qual a criptografia quântica foi criada.

3.1.1 Criptografia de Chave Simétrica

A situação em que as partes de um sistema de comunicação utilizam a mesma chave criptográfica nos processos de cifragem e decifragem é conhecida como criptografia de chave simétrica ou criptografia de chave secreta [3]. Há diversos sistemas de criptografia de chave simétrica, mas um que merece atenção é o proposto por Gilbert Vernam, conhecido

[1] Para o processo de criptografia de chave assimétrica não há necessidade de que as chaves sejam iguais ou conhecidas por ambas as partes.

como chave de uso único ou cifra de Vernam (em inglês é conhecido como *one-time pad*) [34].

A cifra de Vernam é um processo de cifragem definido sobre um alfabeto binário. Uma mensagem binária $M_1M_2\cdots M_t$ é cifrada com a utilização de uma chave binária de mesmo tamanho, produzindo o texto cifrado $C_1C_2\cdots C_t$, em que

$$C_i = \mathrm{Enc}_{k_i}\{M_i\} = M_i + k_i(mod2), \tag{3.5}$$

$1 \leqslant i \leqslant t$ e mod é a operação módulo[35].

A grande vantagem da cifra de Vernam, que foi demonstrada por Claude Shannon [7], é que este algoritmo de cifragem é seguro quando a chave usada é gerada aleatoriamente, tem o mesmo tamanho da mensagem e é utilizada apenas uma vez. Um problema desse método é a necessidade de distribuição dessa chave secreta sem que a espiã tenha informação sobre a mesma, felizmente esse impasse é eliminado com a utilização da criptografia quântica.

3.2 Criptografia Quântica

Foi mostrado que a cifra de Vernam consiste de uma técnica de criptografia clássica com segurança demonstrada formalmente [7]. Contudo, o problema de se estabelecer uma longa chave criptográfica e a distribuição desta chave para ambas as partes, requisito fundamental para a segurança do método a ser utilizado em um cenário prático, parece pouco viável. Porém, as propriedades de sistemas quânticos podem ser utilizadas com o objetivo de sobrepor esses empecilhos.

Uma das características que fazem com que a utilização de sistemas quânticos na transmissão de informação em criptografia traga resultados interessantes é o princípio de indeterminação de Heisenberg, que impõe que a medida simutânea de algumas quantidades de sistemas quânticos possui uma indeterminação inevitável e impossível de se abster [36, 24]. Outro fato importante, advindo de sistemas quânticos, é o teorema da não-clonagem [22]. Ele estabelece que é impossível copiar com perfeição estados quânticos não ortogonais. Essas duas propriedades foram os fundamentos para o desenvolvimento de um novo método de distribuição de chave secreta que será explicado na subseção a seguir.

3.2.1 Protocolos de Distribuição Quântica de Chave Secreta

A criptografia quântica consiste em um método de distribuição quântica de chave secreta seguro, mesmo quando uma possível espiã possui capacidade tecnológica ilimitada,

incluindo a presença de um computador quântico [22]. O primeiro protocolo de criptografia quântica foi proposto em 1984 por C. Bennett e G. Brassard, frequentemente referenciado na literatura como BB84 [11]. Sua proposta inicial utilizou estados polarizados da luz como unidade básica para a distribuição das chaves.

Artur Ekert propôs, em 1991, o protocolo E91 [37], que tem como base o emaranhamento ou correlação quântica de fótons [36]. De acordo com o paradoxo EPR [38], um sistema de dois fótons emaranhados correspondem, do ponto de vista da mecânica quântica, a uma partícula só, de forma que se um dos dois fótons for medido, o outro será também alterado no exato momento da medida, independente de quão distantes eles estejam, isso implica em um método para detectar a presença de espião na rede. O protocolo E91 possui três estágios onde os fótons emaranhados são distribuídos para Alice e para Bob. Uma das partes mede o fóton, em alguma base, e então as duas partes se comunicam por um canal clássico público informando em qual base foi feita a medida. O conjunto de bits é dividido em dois, um que corresponderá à chave secreta criada e a outra parte que será descartada por causa da não correspondência entre as bases medidas por Alice e Bob. No canal público, Alice e Bob comparam os bits que foram descartados e, se eles seguirem a desigualdade de Bell [36], então eles sabem que existe um espião no canal e abortam a transmissão da informação.

Por fim, foi proposto por Eduin, em 2013, o protocolo S13 [39]. Esse protocolo usa reconciliação de uma semente aleatória e da criptografia assimétrica. Comparado com o BB84, onde o percentual de coincidências no processo de reconciliação para a geração de chave é em torno de 50%, o protocolo S13 pode chegar a 100%. Outros protocolos existentes são apresentados e comparados na Tabela 1.

Tabela 1 – Uma comparação de vários protocolos para QKD

Ano	Nome do Protocolo	Princípio em que se baseia	Observação	Referência
1984	BB84	Princípio de indeterminação de Heisenberg	A polarização dos fótons é usada para codificação da informação em quatro estados quânticos.	[11]
1991	E91	Emaranhamento quântico	Pares de fótons emaranhados são usados no lugar da polarização.	[37]
1992	BB92	Princípio de indeterminação de Heisenberg	Similar ao BB84, mas com o uso de apenas dois estados.	[40]
1999	SSP	Princípio de indeterminação de Heisenberg	Usa 6 estados: $\pm x$, $\pm y$ e $\pm z$ na esfera de Bloch.	[41]
2001	Cerf01	Princípio de indeterminação de Heisenberg	A informação é contínua e é armazenada no valor médio do estado comprimido	[33]
2002	GG02	Princípio de indeterminação de Heisenberg	A variável aleatória a compor a chave tem distribuição contínua e o seu envio é feito com a utilização de estados coerentes da luz	[42]
2003	DPS	Emaranhamento quântico	Possui uso eficiente do domínio do tempo e apresenta robustez em ataques de divisão do número de fótons [43] (ou PNS, do inglês *Photon Number Splitting attack*).	[44, 45]
2004	SARG04	Princípio de indeterminação de Heisenberg	Fornece mais segurança que o BB84 contra ataques por divisão do número de fótons.	[46]
2004	COW	Emaranhamento quântico	A utilização deste protocolo é possível quando há alta taxa de bits em pulsos coerentes fracos. Ele possui maior segurança para ataques PNS.	[47, 48]
2009	KMB09	Princípio de indeterminação de Heisenberg	Neste protocolo Alice e Bob codificam o 0 e o 1 em duas bases, ao invés de usar duas direções diferentes em uma base para a codificação da informação.	[49]
2012	S09	Criptografia de chave pública e privada	Pode distribuir chaves entre n sistemas, tendo um sistema central de transmissor da mensagem.	[50]
2013	S13	Princípio de indeterminação de Heisenberg	Usa semente aleatória, não possui perda de informação e diferencia do protocolo BB84 apenas na parte de comunicação pelo canal clássico.	[39]
2014	Jouguet14	Princípio de indeterminação de Heisenberg	Utiliza a ideia do protocolo proposto no GG02 [42] com a adição, na parte de reconciliação, de códigos LDPC de forma a conseguir mais de 1 bit de chave secreta por uso do canal.	[51]

O BB84 continua sendo um dos protocolos de criptografia quântica mais pesquisados e desenvolvidos atualmente. Visando isso e uma abordagem voltada para um melhor entendimento do que é criptografia quântica, será feita uma apresentação do protocolo BB84 e os principais conceitos utilizados por eles no estabelecimento de uma chave criptográfica. Posteriormente, o protocolo proposto por Cerf, et al. [33], utilizando estados comprimidos, também será mostrado, porém com menos detalhes.

3.2.2 Protocolo BB84

Este protocolo foi elaborado por Charles Bennett e Gilles Brassard em 1984 [11] e é baseado no princípio de indeterminação de Heisenberg [24]. Ele foi originalmente descrito usando polarização de fótons para a transmissão da informação, porém implementações práticas em fibras ópticas usam mais a codificação da informação na fase do estado [52]. Esse protocolo é certamente o mais conhecido e mais implementado dentre os protocolos de criptografia quântica. A prova de segurança desse protocolo, contra estratégias de um espião, foram feitas por Shor e Preskill [53].

O transmissor e o receptor, conhecidos como Alice e Bob, respectivamente, estão conectados por um canal quântico de comunicação no qual permite a transmissão de estados quânticos por ele. Nesse canal pode haver uma espiã, Eva, que pode visualizar qualquer transmissão pelo canal. Além disso, Alice e Bob também se comunicam por um canal clássico público. Nenhum desses canais precisam ser seguros, pois o protocolo é construído de forma a prevenir a interferência de Eva sobre qualquer um deles.

Implementações práticas do BB84, tal como a que está sendo feita no Laboratório de Comunicações Quânticas (LCQ) do IQuanta – UFCG, usam mais a codificação em fase, por tornar o sistema de QKD mais robusto a eventos do ambiente quando comparado com o de polarização [52]. Porém, para um melhor entendimento do protocolo, será explicado logo a seguir o BB84 com a utilização de codificação por polarização:

- Base $\oplus$ de polarização horizontal (0°) e vertical ($+90^\circ$). A representação dos estados nessa base é feita como sendo $|0\rangle$ para a polarização horizontal e $|1\rangle$ para a polarização vertical assim, tem-se $\oplus = \{|0\rangle, |1\rangle\}$.
- Base $\otimes$ com polarizações ($+45^\circ$) e ($+135^\circ$). Os estados nessa base são denotados por $|+\rangle$ e $|-\rangle$ para as polarizações ($+45^\circ$) e ($+135^\circ$), respectivamente, ou seja, $\otimes = \{|+\rangle, |-\rangle\}$. Eles também podem ser decompostos nos estados $|0\rangle$ e $|1\rangle$ da seguinte forma [22]

$$|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \tag{3.6}$$

$$|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle). \tag{3.7}$$

Nesse protocolo, a associação entre o bit de informação e o estado de cada base é descrita na Tabela 2.

O protocolo BB84 pode ser descrito da seguinte forma:

1. Transmissão quântica (Primeiro Passo)

Tabela 2 – Esquema de codificação para o protocolo BB84

Bit	$\oplus$	$\otimes$
0	$\|0\rangle = a_{00}$	$\|+\rangle = a_{10}$
1	$\|1\rangle = a_{01}$	$\|-\rangle = a_{11}$

a) Alice escolhe aleatoriamente uma sequência de bits $d \in \{0,1\}^n$ e uma sequência aleatória de bases $b \in \{\oplus, \otimes\}^n$.

b) Ela prepara um fóton no estado a_{ij} para cada bit d_i de d e b_j em b como na Tabela 2, e o envia para Bob pelo canal quântico.

c) Bob escolhe aleatoriamente se vai medir na base $\oplus$ ou $\otimes$ para cada um dos a_{ij} recebidos. A medida de Bob produz uma sequência $d' \in \{0,1\}^n$, quando a escolha da base de medida for $b' \in \{0,1\}^{n2}$.

2. Discussão Pública (Segundo Passo)

a) Para cada bit d_i em d:

i. Alice envia pelo canal clássico o valor de b_i para Bob.

ii. Bob responde a Alice dizendo em quais bits ele usou a mesma base de medida. Os valores de d_i e d'_i são descartados se $b_i \neq b'_i$.

Alice escolhe aleatoriamente um subconjunto dos bits restantes em d e informa a Bob os seus valores pelo canal clássico. Se os resultados da medida de Bob, para uma certa fração de bits, não coincidirem, então pode haver a ação de um espião e a comunicação é abortada.

b) Caso a comunicação não seja abortada, a sequência dos bits restantes em d é usada para criar a chave secreta comum entre Alice e Bob, $k = \{0,1\}^N$ (onde $N < n$).

O entendimento do protocolo BB84 pode ser feito a partir da ideia de medida em mecânica quântica [22]. Se um qbit $|\psi\rangle$ for medido na base ortonormal $\{|c\rangle, |g\rangle\}$, então com probabilidade $|e|^2$ será obtido o estado $|c\rangle$ e $|f|^2$ o estado $|g\rangle$, onde $|e|^2 + |f|^2 = 1$. Consequentemente, a medida com bases incorretas produzirá resultados aleatórios, como predito pela mecânica quântica [22]. Assim, se Bob escolher a base $\otimes$ para medir um fóton no estado $|1\rangle$, o resultado clássico da medida será 0 ou 1 com probabilidade 1/2 para os dois casos, pois

$$|1\rangle = \frac{1}{\sqrt{2}}(|+\rangle - |-\rangle). \tag{3.8}$$

[2] A notação $\{0,1\}^2$ representa uma sequência de n bits

Porém, se a base de Bob for $\oplus$, a saída clássica será sempre 1, pois $|1\rangle = 1\,|1\rangle + 0\,|0\rangle$.

Para detectar Eva, Alice e Bob medem a taxa que, mesmo que a escolha das suas bases sejam idênticas, ou seja, $b_i = b'_i$, os bits não são iguais, $d_i \neq d'_i$. Observe que a não igualdade entre os bits pode ter sido causada pelo ruído do canal e não pela ação propriamente dita de Eva [40].

Um ataque criptográfico é um método para contornar a segurança de um sistema criptográfico através de encontrar fraqueza em um código, cifra, esquema de gerenciamento de chaves ou no protocolo de troca de chaves [3]. Eva pode fazer vários tipos de ataques em um sistema que efetue o QKD [10]. Um dos possíveis ataques é o ataque intercepta-reenvia, onde Eva mede o fóton enviado por Alice e envia um fóton que corresponde ao resultado da sua medida para Bob. Isto produz erro na chave compartilhada entre Alice e Bob. Como Eva não tem conhecimento sobre a polarização dos fótons enviados por Alice, Eva pode apenas supor quais as bases na medida, da mesma forma que Bob. Nos casos onde ela escolhe corretamente a base, ela mede a correta polarização do fóton enviado por Alice e transmite para Bob uma cópia correta do estado. Mas quando a sua escolha de base não é a correta, o estado que ela efetua a medida é uma sobreposição dos possíveis estados gerados nesta base incorreta, o que leva ao estado que Eva transmite para Bob ser algumas vezes diferente do estado que Alice produziu. Se Bob então medir esse estado na base que Alice enviou, a sua saída do medidor pode ser qualquer valor referente à base que ele está medindo, levando a obter valores aleatórios na medida ao invés de resultados corretos por causa da presença de Eva. Uma ilustração deste tipo de ataque é mostrada na Tabela 3.

Tabela 3 – Exemplo do ataque intercepta-reenvia

Bits aleatórios gerados por Alice	0	1	1	0	1	0	0	1
Escolha aleatória de Alice das bases de transmissão	$\oplus$	$\oplus$	$\otimes$	$\oplus$	$\otimes$	$\otimes$	$\otimes$	$\oplus$
Estados enviados por Alice	$\|0\rangle$	$\|1\rangle$	$\|-\rangle$	$\|0\rangle$	$\|-\rangle$	$\|+\rangle$	$\|+\rangle$	$\|1\rangle$
Base aleatória de medida de Eva	$\oplus$	$\otimes$	$\oplus$	$\oplus$	$\otimes$	$\oplus$	$\otimes$	$\oplus$
Polarizações medidas e enviadas por Eva	$\|0\rangle$	$\|+\rangle$	$\|1\rangle$	$\|0\rangle$	$\|-\rangle$	$\|1\rangle$	$\|+\rangle$	$\|1\rangle$
Base aleatória de medidas de Bob	$\oplus$	$\otimes$	$\otimes$	$\otimes$	$\oplus$	$\otimes$	$\oplus$	$\oplus$
Polarizações medidas por Bob	$\|0\rangle$	$\|+\rangle$	$\|+\rangle$	$\|-\rangle$	$\|1\rangle$	$\|+\rangle$	$\|0\rangle$	$\|1\rangle$
Discussão Pública das Bases								
Chave secreta compartilhada	0	–	0	–	–	0	–	1
Erros na chave	✓	–	✗	–	–	✓	–	✓

Eva escolhe uma base incorreta com probabilidade $0,5$, e se Bob medir este fóton interceptado na base que Alice envia, então ele obtém um resultado aleatório na medida, ou seja, um resultado incorreto com probabilidade $0,5$. A probabilidade para cada fóton de interceptá-lo e de gerar um erro na sequência de bits da chave é de $0,5 \times 0,5 = 0,25$, se Eva medir todos os fótons transmitidos por Alice. Se Alice e Bob compararem publicamente n bits da chave, eles detectarão a presença de Eva com probabilidade $1 - (3/4)^n$ [22].

3.2.2.1 Protocolo BB84 em Canais com Ruído

A detecção de um espião, quando se utiliza o protocolo BB84, é feita por meio da verificação da existência de uma taxa de erro nos bits da chave final. Contudo, uma questão importante é que, em um cenário prático, haverá sempre a inserção de erros na comunicação, devido a perdas aleatórias de polarização do fóton ou outros motivos, mesmo quando não há espião. Contudo, a distinção entre erros provocados pelo meio e aqueles oriundos de uma tentativa de espionagem pode ser realizada quando se considera que a taxa de erro de bits ($QBER$) típico alcançado na implementação do protocolo BB84 é menor que 5%. Formalmente, as técnicas de implementação devem possuir uma taxa de erro abaixo do limiar de 25%. Em casos práticos, para evitar falsas detecções de espião, é exigido uma taxa de erro não superior a 10% [9].

Um cenário ainda mais realista é representado pela situação em que Eva obtém apenas uma fração da chave. Na situação apresentada anteriormente, Eva interfere no canal quântico e obtém 50% da informação transmitida, gerando uma QBER de $\approx 25\%$. Se Eva, contudo, interferir em apenas 10% dos qbits enviados por Alice, sua ação irá gerar uma QBER de apenas $\approx 2,5\%$, valor que pode se passar por ruído devido ao canal. Nesse caso, sua presença não será detectada como uma tentativa de espionagem, sendo que Eva obtém apenas $\approx 5\%$ da informação transmitida por Alice. Dessa forma, Eva terá uma sequência, que mesmo fracamente, estará correlacionada à chave k de Alice e Bob.

Para tornar o método mais eficiente, dois procedimentos são realizados com a sequência de bits da chave, os procedimentos de reconciliação da informação e de amplificação de privacidade. O processo de reconciliação da informação executa a correção de erros para as sequências de Alice e Bob e o processo de amplificação de privacidade diminui a informação que foi parar nas mãos de Eva. Esses procedimentos são fundamentais para a inserção do protocolo BB84 em cenários práticos [9], tendo seu funcionamento detalhado nas seções a seguir.

3.2.2.2 Reconciliação da Informação

O procedimento de reconciliação da informação é um processo de correção de erros interativo que é feito sobre o canal clássico com o intuito de diminuir a diferença entre as sequências de Alice e Bob causada pela existência de erros no canal quântico. As técnicas de correção de erros conhecidas exigem a manipulação de parte da informação a ser corrigida, o que no caso do protocolo quântico implica no anúncio dessa informação no canal público. Esse fato implica que Eva ganhará alguma informação referente à chave no processo de correção de erros. Assim, o protocolo BB84 exige que na etapa de reconciliação da informação seja utilizado um método de correção de erros que necessite do mínimo de divulgação de informação.

Algumas técnicas foram propostas desde o surgimento do BB84, sendo algumas discutidas no artigo do Gisin [10]. Contudo, a técnica que apresenta os melhores resultados e vem sendo usada como referência na implementação de protocolos de criptografia quântica consiste no chamado protocolo *cascade*, apresentado inicialmente por Bennet [40], em 1992. O protocolo utiliza a divulgação de alguns bits de paridade relacionados a subconjuntos da chave estabelecida pelo protocolo BB84 em um processo interativo que corrige progressivamente os erros encontrados.

Imagine que a chave que Alice e Bob possuem não seja igual, contendo alguns erros entre elas. Essa chave será denominada de chave bruta. O protocolo *cascade* funciona da seguinte forma. Seja K_i o tamanho do bloco usado no i-ésimo passo do algoritmo. No primeiro passo, as duas partes dividem suas respectivas chaves bruta em blocos de mesmo tamanho. O tamanho K_1 da primeira interação é de acordo com ambas as partes e é calculado como uma função da QBER. No artigo de Bennett [40], é sugerido $K_1 \approx 0,73/QBER$. Posteriormente, as partes calculam as paridades de cada bloco, enviam esse valor por um canal público, mas autêntico, e efetuam uma busca dicotômica quando essas paridades não são iguais. Essa busca objetiva a obtenção do bit em discordância entre Alice e Bob. Nos passos seguintes, o tamanho do bloco é dobrado, $K_i = 2K_{i-1}$, e o processo de troca de paridades e de busca e correção do erro é repetido.

3.2.2.3 Amplificação de Privacidade

A reconciliação da informação permite a Alice e Bob estabelecerem uma chave idêntica, mas apenas parcialmente secreta. O motivo disso é que a informação divulgada na execução do protocolo de correção de erros fornece a Eva alguma informação acerca da chave estabelecida. Adicionalmente, além da informação que Eva obtém do processo de reconciliação, ela pode ganhar alguma informação extra a partir das vulnerabilidades conhecidas de algumas técnicas utilizadas na implementação dos protocolos quânticos.

Entretanto, a técnica conhecida como amplificação de privacidade, introduzida inicialmente por Bennett, et al. [54] permite tornar inútil a informação que Eva obteve acerca da chave, considerando as diferentes fontes de vazamento de informação possíveis. Alice e Bob podem estimar um limitante superior l' para a informação que Eva conseguiu adquirir durante o protocolo de distribuição de chave. O que ela adquiriu na etapa de reconciliação refere-se à paridade de blocos da chave, sendo que em cada etapa do protocolo é considerado que um bit de informação é obtido por Eva, sendo denotado por l''. Assim, a quantidade de bits que Eva possui é $l = l' + l''$. Com essa estimativa, o método de amplificação de privacidade de Bennett, et al. garante que, ao final do algoritmo, a informação que vaza para Eva pode ser tão pequena quanto se deseje. Antes de mencionar o resultado de Bennett, et al. é necessário explicar o que são as funções *hash* propostas por Wegman e Carter [55].

Uma classe $\mathcal{G}$ de funções $\mathcal{A} \rightarrow \mathcal{B}$ é dita *universal*$_2$ se, para qualquer x_1 e x_2 distintos de $\mathcal{A}$, a probabilidade que $g(x_1) = g(x_2)$ é no máximo igual a $1/|\mathcal{B}|$, quando g é escolhida aleatoriamente de $\mathcal{G}$ de acordo com uma distribuição uniforme de probabilidade.

Com isso, o resultado de Bennett, et al. é apresentado a seguir. Considere que a chave bruta W tenha n bits uniformemente distribuídos. Se Eva possui l bits de informação sobre W, então considere a quantidade $r = n-l-s$, onde s é um parâmetro de segurança. Se Alice e Bob escolherem $k = g(W)$ como sendo sua chave secreta, onde g é escolhida aleatoriamente do conjunto de funções *hash universal*$_2$ que tem como domínio $\{0,1\}^n$ e contradomínio $\{0,1\}^r$, então o valor médio da informação final que Eva possui sobre k, dado que ela sabe a função g e possui l bits de informação é

$$I_{Eva}^{final} \leqslant 2^{-s}/ln2. \tag{3.9}$$

Este método de reconciliação é bastante eficaz e usado em diversos protocolos de distribuição de chave.

3.2.2.4 Ataques contra o Protocolo BB84

Imperfeições que ocorrem invariavelmente na implementação do protocolo permitem que alguns ataques possam ser efetuados explorando certas vulnerabilidades. A seguir será apresentado o ataque interceptação-reenvio e *beam-splitting*, por serem considerados os mais importantes para o desenvolvimento deste trabalho.

3.2.2.4.1 Interceptação-Reenvio

Essa é a estratégia de ataque mais acessível à Eva para tentar corromper o protocolo BB84. Nesse ataque Eva recebe os qbits de Alice e realiza uma medição em uma das bases de medida do protocolo, tal como faria Bob. Ela então prepara um qbit no estado igual ao medido por ela e então envia este a Bob. Eva tem uma chance de 50% de realizar a medida correta para o qbit enviado por Alice. Nesse caso, ela também enviará o estado correto a Bob, não sendo assim detectada. Contudo, para os outros 50% das vezes, ela irá causar uma descorrelação entre os resultados de Alice e Bob, o que ajudará Alice e Bob a detectar sua presença. Isso permite a Eva capturar $\approx$ 50% da informação referente à chave trocada por Alice e Bob, produzindo um aumento na taxa de erros de $\approx$ 25%. Contudo, para não ser detectada e tentar confundir os erros causados por ela com os erros intrínsecos do canal quântico, Eva aplica o ataque a apenas uma fração dos qbits enviados por Alice, por exemplo, se atacar sobre 20% dos qbits que Alice enviou, Eva irá gerar uma taxa de erro de somente 5%, com o prejuízo de obter cerca de 10% da informação acerca da chave trocada.

3.2.2.4.2 Ataque *Beam-Splitting*

Outra fonte de obtenção de informação consiste em um ataque que utiliza a imperfeição das implementações físicas do canal quântico para tentar extrair informação acerca da chave trocada por meio do protocolo.

Frequentemente, os geradores de pulso de laser utilizados nas implementações do protocolo BB84 não produzem apenas um fóton por pulso, ocorrendo, ocasionalmente, a produção de mais de um fóton em cada pulso. Esse fóton em excesso pode ser utilizado por Eva por meio de uma técnica de divisão de feixe, o que permite que ela possa realizar uma medição sobre um dos fótons e deixando inalterado o outro que é então enviado a Bob.

A presença de Eva nesse caso é difícil de ser detectada, uma vez que ela não altera o estado dos qbits que chega até Bob. Contudo, nas fontes de fótons atuais, a produção de mais de um fóton por pulso é baixa e sendo caracterizada por uma distribuição de probabilidade tipicamente equivalente à distribuição de Poisson. Isso permite que a informação adquirida por Eva através de um ataque tipo *beam-splitting* possa ser adequadamente tratada no processo de amplificação de privacidade.

3.2.3 Protocolo de Distribuição de Chave Secreta Utilizando Estados Comprimidos da Luz

No protocolo de Cerf, et al. [33], a informação é armazenada em uma das quadraturas X_1 e X_2 do campo eletromagnético, onde essas quadraturas satisfazem a seguinte relação de indeterminação

$$\Delta X_1 \Delta X_2 \geqslant 1/16. \tag{3.10}$$

Isso possibilita a construção do seguinte protocolo. Alice codifica a sua mensagem $m \sim \mathcal{N}(0, \Sigma^2)$ em uma das quadraturas, onde essa escolha da quadratura é feita aleatoriamente. Na quadratura escolhida, ela impõe uma compressão $\Delta X_i^2 = \sigma_i^2 < 1/4$ na variância e coloca o valor médio em $\langle X_i \rangle = m$. Envia para Bob e ele escolhe uma das quadraturas para medir. Alice informa, por um canal público e autêntico, a sequência das quadraturas que ela usou para Bob. Caso as quadraturas que Alice escolheu e Bob mediu sejam iguais, o protocolo é bem sucedido, caso contrário eles descartam o que foi enviado e efetuam o processo novamente.

Para que o protocolo seja seguro, é necessário que as distribuições de X_1, quando Alice sorteia a quadratura 1 ou quando sorteia a quadratura 2, sejam iguais. Para isso,

observe que quando a quadratura 1 é escolhida, tem-se

$$\Delta X_1^2 = \Sigma^2 + \sigma_1^2, \tag{3.11}$$

Sigma corresponde a variância da variável aleatória m gerada por Alice e σ indeterminação com relação à quadratura 1 quando Alice toma como quadratura a ser escrita o valor de m como sendo a 1. Quando a quadratura 2 é escolhida, deve-se manter a relação

$$\Delta X_1^2 \Delta X_2^2 = \frac{1}{16}, \tag{3.12}$$

o que impõe

$$\Delta X_1^2 \sigma_2^2 = \frac{1}{16} \tag{3.13}$$

e

$$\Delta X_1^2 = \frac{1}{16\sigma_2^2}. \tag{3.14}$$

Juntando as informações das Eq. 3.12 e 3.14, obtêm-se

$$\Sigma^2 + \sigma_1^2 = \frac{1}{16\sigma_2^2}. \tag{3.15}$$

Usando o mesmo procedimento, chega-se a

$$\Sigma^2 + \sigma_2^2 = \frac{1}{16\sigma_1^2}. \tag{3.16}$$

O que pode ser usado para produzir as igualdades

$$1 + \frac{\Sigma^2}{\sigma_1^2} = 1 + \frac{\Sigma^2}{\sigma_2^2} = \frac{1}{\alpha^2}, \tag{3.17}$$

onde $\alpha = 4\sigma_1\sigma_2 = e^{-(r_1+r_2)}$, com r_1 e r_2 sendo os parâmetros de compressão das quadraturas 1 e 2, respectivamente.

Para uma situação sem Eva e com o canal sem ruído, Cerf, et al. mostraram que a informação mútua entre Alice e Bob para esse protocolo é igual a

$$I_{AB}^{Sem\ Eva} = -\log_2(\alpha) = (r_1 + r_2)/ln2 = \log_2(2\langle N\rangle + 1), \tag{3.18}$$

onde $\langle N\rangle$ é o número médio de fótons do estado comprimido utilizado.

Por fim, se Eva possui uma máquina de clonagem ótima e só faz a medida depois de Alice dizer as bases utilizadas, eles mostraram que a informação mútua entre Alice e Bob será

$$I_{AB}^{Com\ Eva} = \frac{1}{2}\log_2\left(\frac{1+\alpha\chi\lambda}{\alpha^2+\alpha\chi\lambda}\right) \tag{3.19}$$

e a entre Alice e Eva

$$I_{AE} = \frac{1}{2}\log_2\left(\frac{1+\alpha/(\chi\lambda)}{\alpha^2+\alpha/(\chi\lambda)}\right), \tag{3.20}$$

onde χ e λ são parâmetros relacionados com as variâncias do estado produzido pela máquina de clonagem. Esse protocolo garante a transmissão segura de uma chave criptográfica se

$$\gamma' > \sqrt{1+\gamma} - 1, \tag{3.21}$$

onde γ e γ' são as SNRs sem e com Eva, respectivamente.

Grosshans e Grangier [42] ampliaram o trabalho feito por Cerf [33]. Eles estudaram a segurança do protocolo de Cerf sobre a ação de Eva aplicando o ataque *beam-splitteing*. Eles consideraram a seguinte descrição de ataque: se o ruído do canal notado por Bob é dado por χN_0, onde N_0 é a variância do ruído do vácuo, então Eva substitui esse meio de transmissão por um sem perdas e coloca um *beam-sppliter* com reflexividade $1-\eta$, onde $\chi = (1-\eta)/\eta$ e η é a reflexibilidade do *beam-sppliter*. Com isso, Bob não notará a presença de Eva, pois o canal se comportará da mesma forma que anteriormente.

Por fim, eles mostraram que a condição para construção de uma chave segura é ter $\chi < 1$, ou $\eta > 1/2$. Uma comparação que será feita no Capítulo 5 é que o protocolo que foi criado não apresenta essa necessidade. Mesmo com valores de reflexibilidade, ainda há a possiblidade de criação de uma chave secreta, necessitando apenas que se aplique uma maior compressão sobre o estado comprimido bimodal que é utilizado no protocolo.

Os protocolos de reconciliação e de amplificação de privacidade para QKD utilizando variáveis contínuas não serão explicados. O motivo disso é que normalmente se utiliza os já consolidados que foram, inicialmente, criados para QKD de variáveis discretas, havendo apenas a necessidade de discretização e codificação dos valores obtidos depois da "parte quântica" do QKD.

Para terminar a fundamentação teórica mínima necessária para o entendimento do protocolo criado, no Capítulo 4 será explicado o que é modulação não linear (ou mapas de Shannon-Kotel'nikov) e alguns métodos de demodulação, que poderiam ser utilizados em trabalhos futuros para uma melhor descrição matemática da forma de medida de Bob no protocolo do Capítulo 5.

4 Métodos de Modulação Linear e Não Linear

Neste capítulo será mostrada uma abordagem geométrica de esquemas de modulação. Inicialmente, a relação entre a modulação e o espaço de sinais é vista brevemente, seguido dos métodos de modulação linear e não linear. Essas técnicas de modulação não lineares serão utilizadas, de modo inédito, até o que conhecemos, para preparar estados quânticos em um esquema de distribuição quântica de chaves secretas (QKD) de variáveis contínuas.

4.1 Modulação Linear

O uso de modulações lineares surgiu desde o início das comunicações. Eles se destacaram com o uso da modulação AM e seus derivados, e. g., DSB, DSB-SC, etc. É essa classe de modulação que será apresentada a seguir e que servirá como base para o decorrer do trabalho.

4.2 Transmissão de um Único Parâmetro

A fonte de informação que está sendo estudada é uma variável aleatória contínua, ou seja, a fonte gera números reais aleatoriamente dentro ou não de uma faixa de valores. Sendo assim, considere o sistema de comunicação ilustrado na Fig. 3. A forma de onda que é transmitida é

$$s_m(t) = mA\varphi_1(t), \tag{4.1}$$

onde m representa a fonte de informação, A é o ganho de um amplificador na transmissão e $\varphi_1(t)$ é alguma forma de onda com energia unitária,

$$\int_{-\infty}^{\infty} \varphi_1^2(t)dt = 1. \tag{4.2}$$

Ao transmitir o sinal, ele é afetado por um processo aleatório Gaussiano ruídoso $n_w(t)$ que possui densidade espectral de potência igual a $N_0/2$ e que é introduzido no canal. Ou seja, o sinal na saída do canal é dado por

$$r(t) = s_m(t) + n_w(t). \tag{4.3}$$

Será analisado o sistema sobre várias formas de otimização do sinal recebido.

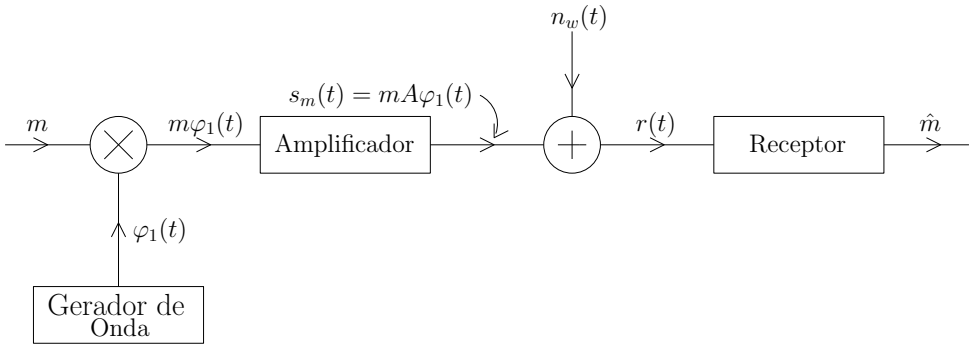

Figura 3 – Sistema simples de modulação linear para a transmissão de uma variável aleatória m.

4.2.1 Receptor de Menor Erro Médio Quadrático

A construção desse receptor é feita sobre a consideração a ter, na saída do mesmo, o menor erro médio quadrático. Primeiramente, considere que o processo recebido $r(t)$ é representado por algum vetor $\boldsymbol{r}$. Para ter um erro médio quadrático total mínimo, é necessário e suficiente que a minimização seja feita sobre $\overline{\epsilon^2}(\boldsymbol{\rho})$, dado cada possível valor de $\boldsymbol{\rho}$ do vetor recebido $\boldsymbol{r}$. Isso segue do fato que o erro médio quadrático total pode ser escrito como

$$\overline{\epsilon^2} = \int_{-\infty}^{\infty} \overline{\epsilon^2}(\boldsymbol{\rho}) p_r(\boldsymbol{\rho}) d\boldsymbol{\rho}, \tag{4.4}$$

com

$$\begin{aligned} \overline{\epsilon^2}(\boldsymbol{\rho}) &= \int_{-\infty}^{\infty} (\alpha - \hat{m})^2 p_m(\alpha | \boldsymbol{r} = \boldsymbol{\rho}) d\alpha & (4.5) \\ &= E[(m - \hat{m})^2 | \boldsymbol{r} = \boldsymbol{\rho}]. & (4.6) \end{aligned}$$

É possível mostrar que o melhor valor do estimador que diminui o erro médio quadrático é $\hat{m} = \bar{m}(\rho)$ [16]. Assim, é necessário calcular

$$\overline{\epsilon^2}(\boldsymbol{\rho}) = E[(m - \bar{m})^2 | \boldsymbol{r} = \boldsymbol{\rho}]. \tag{4.7}$$

Para exemplificar o cálculo do receptor, considere que o canal é AWGN. Isso leva a

$$r_1 = \boldsymbol{r} \cdot \boldsymbol{\varphi_1} = \int_{-\infty}^{\infty} r(t)\varphi_1(t)dt = \int_{-\infty}^{\infty} (s_m(t)\varphi_1(t) + n_w(t))\varphi_1(t)dt = mA + n_1 \tag{4.8}$$

onde n_1 denota a componente do ruído na direção do vetor $\varphi_1(t)$. Com isso, o estimador é

$$\overline{m} = \overline{m}(\rho) = \int_{-\infty}^{\infty} \alpha p_m(\alpha|r_1 = \rho)d\alpha \tag{4.9}$$

e o resultado do erro médio quadrático será

$$\overline{\epsilon^2}(\boldsymbol{\rho}) = E[(m - \overline{m}(\rho))^2|r_1 = \rho]. \tag{4.10}$$

Observando que

$$p_m(\alpha|r_1 = \rho) = \frac{p_m(\alpha)}{p_{r_1}(\rho)} p_{r_1}(\rho|m = \alpha) \tag{4.11}$$

e

$$p_{r_1}(\rho|m = \alpha) = p_{n_1}(\rho - \alpha A) = \frac{1}{\sqrt{\pi N_0}} e^{-(\rho - \alpha A)^2/N_0}, \tag{4.12}$$

então

$$p_m(\alpha|r_1 = \rho) = B_1 p_m(\alpha) e^{-(\rho - \alpha A)^2/N_0}, \tag{4.13}$$

onde B_1 é uma constante de normalização. Agora, considere que m seja uma variável aleatória gaussiana com fdp (função densidade de probabilidade) igual a

$$p_m(\alpha) = \frac{1}{\sqrt{2\pi}\sigma} e^{-\alpha^2/2\sigma^2}. \tag{4.14}$$

Para este caso, a probabilidade $p_m(\alpha|r_1 = \rho)$ será

$$p_m(\alpha|r_1 = \rho) = B_2 \exp\Big[-\frac{1}{2} \frac{A^2\sigma^2 + N_0/2}{\sigma^2 N_0/2} \Big(\alpha - \rho \frac{\sigma^2 A}{\sigma^2 A^2 + N_0/2}\Big)^2 \Big], \tag{4.15}$$

onde

$$B_2 = \frac{1}{\sqrt{2\pi}} \Big(\frac{\sigma^2 N_0/2}{A^2\sigma^2 + N_0/2} \Big)^{1/2}. \tag{4.16}$$

A média condicional para este caso é

$$\overline{m}(\rho) = \frac{\rho}{A} \frac{1}{1 + \frac{N_0/2}{\sigma^2 A^2}} \tag{4.17}$$

e o erro médio quadrático

$$\overline{\epsilon^2}(\rho) = \frac{\sigma^2 N_0/2}{A^2\sigma^2 + N_0/2} \tag{4.18}$$

$$= \sigma^2 \frac{1}{1 + \frac{\sigma^2 A^2}{N_0/2}}. \tag{4.19}$$

Notando que

$$\overline{E}_m = E\Big[\int_{-\infty}^{\infty} s_m^2(t)dt\Big] = A^2\overline{m^2} = \sigma^2 A^2, \tag{4.20}$$

e que $\overline{\epsilon^2}(\rho)$ não depende de ρ, então

$$\overline{\epsilon^2} = \overline{m^2}\frac{1}{1 + 2\overline{E}_m/N_0}. \tag{4.21}$$

Note que, quando $\overline{E}_m/N_0 \to \infty$, o erro médio quadrático tende a zero, caso em que a comunicação entre o transmissor e o receptor é perfeita.

4.2.2 Receptor de Máxima Verossimilhança

Um receptor de máxima verossimilhança é um receptor que associa ao representante $\hat{m}$ o valor de m tal que

$$p_r(\boldsymbol{\rho}|m = \hat{m}) \geqslant p_r(\boldsymbol{\rho}|m = \alpha), \tag{4.22}$$

para todos os possíveis valores de α. Para o caso de modulação linear com o ruído do canal sendo AWGN, tem-se que

$$p_r(\boldsymbol{\rho}|m = \alpha) \sim p_{r_1}(\rho|m = \alpha) \tag{4.23}$$

$$= \frac{1}{\sqrt{\pi N_0}} e^{-(\rho - \alpha A)^2/N_0}. \tag{4.24}$$

Assim, como o valor de α que maximiza o lado direito da Eq. (4.24) é ρ/A, então

$$\hat{m} = \frac{\rho}{A}. \tag{4.25}$$

Para esse caso que está sendo descrito, o erro médio quadrático pode ser calculado da seguinte forma

$$\hat{m} = (mA + n_1)\frac{1}{A} = m + \frac{n_1}{A} \tag{4.26}$$

$$\overline{\epsilon^2} = \overline{(m - \hat{m})^2} = \frac{N_0}{2A^2}. \tag{4.27}$$

Como $A^2 = \bar{E}_m/m^2$, então

$$\frac{Sinal}{Ruído} = \frac{S}{N} = \frac{2\bar{E}_m}{N_0}. \tag{4.28}$$

4.3 Transmissão de Vários Parâmetros

Será apresentada uma generalização do que foi visto para o caso em que o transmissor envia várias amostras da mesma variável aleatória m, ou seja, considere que se tenha

$$\boldsymbol{m} = (m_1, m_2, ..., m_K), \tag{4.29}$$

onde cada m_i é uma amostra da mesma variável aleatória m. Tendo esses valores, é feito o envio dessas amostras através do uso de uma base $\{\varphi_k\}$ de funções ortonormais para cada valor, isso leva a

$$s_{\boldsymbol{m}} = A\sum_{k=1}^{K} m_k\varphi_k(t). \tag{4.30}$$

O objetivo da construção do receptor é extrair dos valores recebidos a melhor estimativa, $\hat{\boldsymbol{m}} = (\hat{m}_1, ..., \hat{m}_K)$, do vetor transmitido.

Como no caso anterior, tem-se que o sinal recebido é perturbado por um ruído $n_w(t)$ de forma que

$$r(t) = s_m(t) + n_w(t), \tag{4.31}$$

onde se terá $\boldsymbol{r} = (r_1, ..., r_K)$ como o sinal recebido no espaço de sinais e

$$\begin{aligned} r_k &= \int_{-\infty}^{\infty} r(t)\varphi_k(t)dt & (4.32)\\ &= m_kA + n_k, & (4.33) \end{aligned}$$

para $k = 1, 2, ..., K$. Considerando que $n_w(t)$ representa um ruído branco gaussiano, então

$$\begin{aligned} p_r(\boldsymbol{\rho}|\boldsymbol{m} = \boldsymbol{\alpha}) &= \frac{1}{(\pi N_0)^{K/2}} e^{-|\boldsymbol{\rho}-\boldsymbol{\alpha}A|^2/N_0} & (4.34)\\ &= \prod_{k=1}^{K} \frac{1}{\sqrt{\pi N_0}} e^{-(\rho_k-\alpha_kA)^2/N_0}. & (4.35) \end{aligned}$$

Essa equação implica que os valores do vetor $\boldsymbol{\alpha}$ que maximiza $p_r(\boldsymbol{\rho}|\boldsymbol{m} = \boldsymbol{\alpha})$ são $\{\alpha_k = \rho_k/A\}$, para $k = 1, ..., K$. Assim, o receptor de máxima verossimilhança estima os parâmetros m_k's dos valores recebidos ρ_k's da seguinte forma

$$\hat{m}_k = \frac{\rho_k}{A}, \tag{4.36}$$

para $k = 1, 2, ..., K$.

Uma medida apropriada da performance da comunicação de um vetor aleatório de parâmetros é o erro médio quadrátrico por componente, no qual será

$$\begin{aligned} \overline{\epsilon^2} &= \frac{1}{K} E[|\boldsymbol{m} - \hat{\boldsymbol{m}}|^2] && (4.37)\\ &= \frac{1}{K} \sum_{k=1}^{K} \overline{(m_k - \hat{m}_k)^2} && (4.38)\\ &= \frac{N_0}{2A^2}. && (4.39) \end{aligned}$$

Observe que, na última igualdade, foram usados os resultados encontrados anteriormente.

4.4 Modulação Não Linear

Considere o sistema de comunicação ilustrado na Fig. 4, onde $n(t)$ é o ruído aditivo do canal, $r(t)$ é o sinal recebido e $\hat{m}$ é a estimativa que é feita na recepção com relação a m. A fonte de informação que está sendo estudada é uma variável aleatória contínua e m é uma realização dela, ou seja, a fonte transmite números reais aleatoriamente dentro ou não de uma faixa de valores limitados, com função densidade de probabilidade *a priori* p_m. A forma de onda que é transmitida é dada por

$$s_m(t) = s_1(m)\varphi_1(t) + s_2(m)\varphi_2(t) + \cdots + s_N(m)\varphi_N(t), \tag{4.40}$$

onde $\varphi_i(t), i = 1, \cdots, N$ são funções ortogonais com energia unitária e $s_j(m), j = 1, \cdots, N$ é a parametrização de $s_m(t)$ na base $\{\varphi_i(t)\}$.

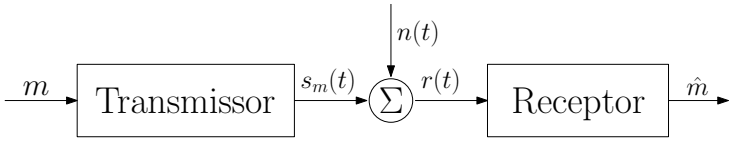

Figura 4 – Diagrama de blocos do sistema de comunicação considerado.

A Eq. (4.40) pode ser reescrita em notação vetorial equivalente

$$\begin{aligned} \mathbf{s}_m &= s_1(m)\varphi_1 + \ldots + s_N(m)\varphi_N \\ &= \Big(s_1(m), \ldots, s_N(m)\Big). \end{aligned} \tag{4.41}$$

Note que com a notação das Eqs. (4.40) e (4.41) é natural estender a técnica de modulação não linear como um mapeamento

$$\begin{aligned} \Re^M &\rightarrow \Re^N \\ \mathbf{m} &\mapsto \mathbf{s_m} \end{aligned} \tag{4.42}$$

no qual m, substituída por $\mathbf{m}$, é interpretada com0 um vetor aleatório $M-$dimensional.

4.4.1 Considerações Geométricas

Considere, para o caso $M = N = 1$, que o lugar geométrico do sinal modulado seja

$$\mathbf{s}_m = mA\varphi_1, \tag{4.43}$$

em que A é uma constante positiva que representa um ganho feito sobre a variável transmitida. Para clareza da explanação, sem perda de generalidade essencial, suponha que a mensagem m seja restrita ao intervalo $[-1, 1]$, então o amplificador no modulador faz um alongamento do sinal transmitido para um intervalo $[-A, A]$ no espaço de sinais, veja Fig. 5. Se esse alongamento for uniforme, então

$$\left|\frac{d\mathbf{s}_m}{dm}\right| = A, \tag{4.44}$$

para todo valor possível de m.

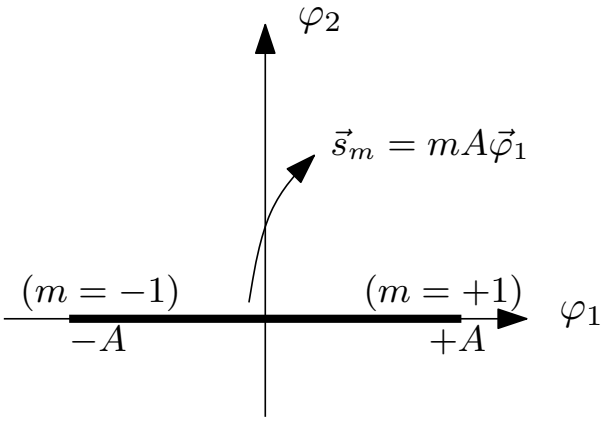

Figura 5 – Lugar geométrico do sinal modulado para m no intervalo $[-1, 1]$.

O efeito do receptor de máxima verossimilhança [16] é desfazer esse alongamento efetuado no transmissor, fazendo com que o sinal volte ao intervalo $[-1, 1]$. É possível mostrar [16] que o erro médio quadrático desse receptor é

$$\overline{\epsilon^2} = \mathbb{E}[(m - \hat{m})^2] = \overline{\left(\frac{n_1}{A}\right)^2} = \frac{N_0}{2A^2}. \tag{4.45}$$

A dependência do $\overline{\epsilon^2}$ sobre a quantidade de alongamento no transmissor é feita explicitamente pela definição de

$$S = \left|\frac{d\mathbf{s}_m}{dm}\right|, \tag{4.46}$$

S é denotado de fator de alongamento. Em termos de S, a Eq. (4.45) é escrita como

$$\overline{\epsilon^2} = \frac{N_0/2}{S^2}. \tag{4.47}$$

4.4.2 Aproximação de Baixo Nível de Ruído

A partir de agora, será analisado brevemente o caso do uso da modulação não linear quando a energia do ruído do canal é pequena comparada com a energia do sinal transmitido. Nele é feito a transmissão de vários valores da fonte de informação, como por exemplo $\mathbf{m} = (m_1, m_2, ..., m_M)$, simultaneamente por meio do uso de diversas funções ortonormais, tais como diversas funções $\varphi_1, \varphi_2, ..., \varphi_N$ com específicas frequências (N e M podem ou não serem iguais, sendo $N > M$ diz-se que está havendo uma imersão). No espaço de sinais, que é o espaço onde é normalmente caracterizado o vetor transmitido e recebido [16], o que é enviado pelo canal é descrito pelo vetor $\mathbf{s}_m$, no qual possui como valor de cada coordenada aquele que é atribuído como amplitude de s_1, s_2, etc. Observe que $\mathbf{s}_m$ é um vetor do espaço de sinais com dimensão N e que depende de M variáveis, $m_1, m_2, ..., m_M$.

Retomando ao caso unidimensional, considere que o parâmetro de entrada do modulador, m, tenha assumido um valor m_0 de forma que $\mathbf{s}_m = \mathbf{s}_0$ e que a densidade do ruído é pequena, a um nível que o ponto recebido, $\mathbf{r}$, esteja próximo $\mathbf{s}_0$ do ponto transmitido. Para esse caso, é possível fazer uma aproximação de primeira ordem sobre o sinal recebido em torno do ponto de interesse $\mathbf{s}_0$, ou seja,

$$\mathbf{s}_m \approx \mathbf{s}_0 + (m - m_0)\dot{\mathbf{s}}_0, \tag{4.48}$$

com

$$\dot{\mathbf{s}}_0 = \left.\frac{d\mathbf{s}_m}{dm}\right|_{m=m_0}. \tag{4.49}$$

Localmente, o problema em que está sendo construído é similar ao problema da modulação linear. Com o ruído branco gaussiano, o receptor de máxima verossimilhança escolhe $\hat{m}$ para m de forma que $|\mathbf{r}-\mathbf{s}_m|$ seja o mínimo possível. Sobre a consideração de um ruído fraco, é possível negligenciar a probabilidade de $\mathbf{r}$ estar em uma região que não esteja próxima do verdadeiro valor transmitido. Na vizinhança de $\mathbf{r}$, a possível região geométrica do sinal recebido se assemelha a um alongamento da região do sinal transmitido por um fator $|\dot{\mathbf{s}}_0|$. Assim, o erro médio quadrático condicional [16] será

$$E[(m-\hat{m})^2|m=m_0] \approx \frac{N_0/2}{|\dot{\mathbf{s}}_0|^2}. \tag{4.50}$$

É frequente que se expresse o fator de alongamento S diretamente em termos de $s_m(t)$. Como a magnitude quadrática de um vetor é igual à sua energia no correspondente tempo, então

$$|\dot{\mathbf{s}}_0|^2 = \int_{-\infty}^{\infty} \Big[\frac{\partial s_m(t)}{\partial m}\Big]^2_{m=m_0} dt. \tag{4.51}$$

Assim, sempre que o lado direito da igualdade anterior for independente de m, é possível definir o fator de alongamento como sendo

$$S^2 = \int_{-\infty}^{\infty} \Big[\frac{\partial s_m(t)}{\partial m}\Big]^2 dt \tag{4.52}$$

e, considerando que o ruído é pequeno, o erro médio quadrático será dado, em termos de S, por

$$\overline{\epsilon^2} = \frac{N_0/2}{S^2}. \tag{4.53}$$

Veja a referência [16] para maiores detalhes.

4.4.3 Observações sobre o Limiar do Ruído

A discussão realizada até esse ponto deixa claro que esquemas de modulação não lineares podem ser vistos como parametrizações de curvas ou superfícies no espaço dos sinais, como pode ser visto pela descrição feita do vetor $\mathbf{s}_m$ transmitido pelo canal ou em mais detalhes na referência [16]. O ruído advindo do canal de comunicação ou de agentes externos, como a tentativa de medição do sinal transmitido pelo canal por um espião, introduz uma variação no sinal transmitido. Quando o ruído ultrapassa um certo valor de limiar, o representante $\hat{m}$ calculado na recepção e comparado com o valor verdadeiro m varia muito.

Considere que a curva que descreve a possível modulação do sinal seja confinada a uma esfera de dimensionalidade fixa e raio $\sqrt{E_s}$. Assim, observe que o comprimento da

curva não pode ser aumentado indefinidamente sem que dois pontos de curvas diferentes estejam muito próximos, veja a Fig. 6. Por outro lado, como indicado pelo círculo tracejado, a função densidade de probabilidade condicional sobre o vetor recebido $\mathbf{r}$, dado $\mathbf{s} = \mathbf{s}_0$, é uma esfera simétrica em torno do ponto transmitido $\mathbf{s}_0$, com o contorno dado por uma densidade de probabilidade que depende da densidade espectral do ruído $N_0/2$. Assim, quando o comprimento L da curva aumenta indefinidamente enquanto E_s e $N_0/2$ são mantidos constantes, vários pontos da curva se aproximam, de forma que a probabilidade de um ponto recebido ser detecctado em outra região seja alta, o que leva a uma anomalia, pois dois pontos próximos correspondem a valores distantes gerados pela fonte.

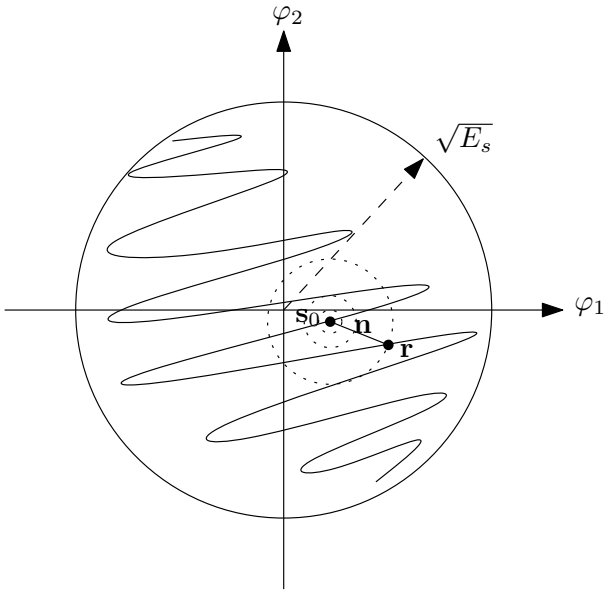

Figura 6 – Lugar geométrico do sinal para o qual a análise linear se torna inválida.

Na verdade, pode-se ver que não só apenas se tem um desvio no sinal transmitido, mas todo o sistema de comunicação falha sobre essa condição de erro. Por exemplo, a saída $\hat{m}$ do receptor de máxima verossimilhança salta descontinuamente com um pequeno valor de ruído, fazendo com que o vetor recebido $\mathbf{r}$ mova continuamente através dos valores ρ_1 e ρ_2 separados na curva e $\hat{m}$ varie de $\mathbf{s}_0$ para $\mathbf{s}_1$. Como a modulação é não linear, os valores $\mathbf{s}_0$ e $\mathbf{s}_1$ são muito distantes, implicando em uma falha no sistema de comunicação por causa dessa descontinuidade dos valores $\hat{m}$ obtidos. Veja a Fig. 7.

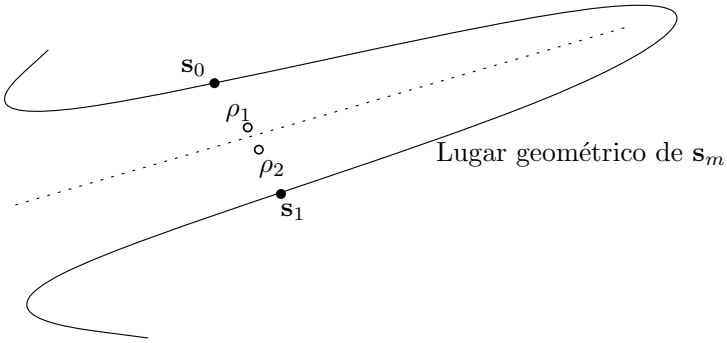

Figura 7 – Quando $\mathbf{r} = \rho_1$, o ponto $\mathbf{s}_m$ de menor distância a $\mathbf{r}$ é próximo a $\mathbf{s}_0$, fazendo com que $\hat{m}$ seja quase igual a m. Isto não é verdade quando $\mathbf{r} = \rho_2$, que corresponde a $\mathbf{s}_1$.

4.4.4 Processo de Demodulação

Existem várias formas de demodulação para o caso não linear, em uma delas é utilizada a tangente da curva relacionada ao esquema de modulação. Porém, o critério de decisão que será usado é o de menor distância entre o ponto recebido e o seu possível representante na curva. Assim, o processo de demodulação pode ser entendido pela seguinte equação

$$\hat{m}(t) = \arg_m \min |s_m(t) - r(t)|. \tag{4.54}$$

Como é possível notar, essa modulação é de simples implementação experimental e de fácil simulação numérica, ajudando a extrair resultados de forma mais simples e rápida sobre a variável requerida. Ele é representado na Fig. 8.

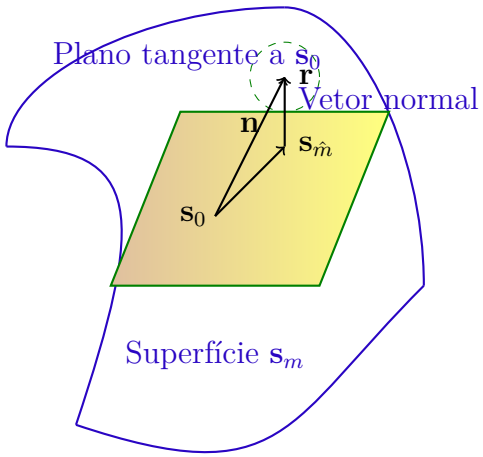

Figura 8 – Recepção por máxima verossimilhança de um sistema de comunicações usando uma modulação não linear quando o ruído tem energia média pequena comparada com a do sinal.

Finalmente, no Capítulo 5 seguinte, será exposto o protocolo criado e analisado. Ele utiliza os conhecimentos presentes nos capítulos anteriores e analisa o protocolo criado por meio do cálculo de informação mútua entre Alice e Bob e entre Ela e Eva.

5 Preparação de Estados Quânticos para QKD com Mapas de Shannon-Kotel'nikov

Nesse capítulo será apresentado o protocolo de distribuição quântica de chave secreta utilizando mapas de Shannon-Kotel'nikov. Em particular, a imagem dos mapas utilizados será curvas construídas sobre toros com quatro dimensões, isso será possível com a utilização do estado comprimido de dois modos.

5.1 Mapas de Shannon-Kotel'nikov

A ideia de usar a geometria de curvas para expansão da largura de banda foi estudada por Shannon [56] e por Kotel'nikov [57]. Nos últimos anos vários autores têm trabalhado nessa área [58, 59, 60, 61, 62]. Os mapas de Shannon-Kotel'nikov são métodos de mapear uma quantidade M de valores contínuos gerados pela fonte em N vetores que serão enviados pelo canal de comunicação. Estudos sobre a otimização do erro médio quadrático mínimo na decodificação [63], a utilização desses mapas para sistemas distribuídos [60], entre outros foram feitos. Em resumo, o que foi mostrado no Cap. 4 é todo o conhecimento que será necessário sobre tais mapas nessa dissertação. Agora, a curva que será utilizada na construção do protocolo para QKD será mostrada.

5.2 Curvas em Camadas de Toro

Foi visto no Cap. 4 que a utilização de mapas de Shannon-Kotel'nikov podem fornecer um método para a redução do erro médio quadrático na transmissão de informação em um canal AWGN (do inglês *Additive White Gaussian Noise*). Além disso, esses mapas podem ser utilizados com o objetivo de compressão, autenticação de usuário, entre outros [58, 59, 60, 61, 62]. Neste trabalho, entretanto, as técnicas de modulação não linear são propostas para a preparação de estados quânticos utilizados em um esquema de distribuição quântica de chave. Até onde vai o conhecimento do autor, essa modalidade de aplicação é inovadora a ponto de não haver nenhum resultado similar. Isto é, não foram encontrados trabalhos com esta proposta durante a revisão bibliográfica, que é apresentada no Cap. 3. Em princípio, qualquer sistema de modulação não linear poderia ser empregado, porém, neste trabalho, a aplicação sera feita com as curvas em camadas de toros detalhadas no trabalho de Antônio Carlos Jr. [61, 64]. Ele propôs diversos métodos de se criar curvas sobre toros, mas apenas uma em particular será utilizada e descrita

aqui. O motivo disso é que esse trabalho tem como objetivo propor um protocolo utilizando mapas de Shannon-Kotel'nikov e não analizar diversos diversos mapas e elencar os melhores.

Essas curvas podem ser definidas da seguinte forma. Seja $\mathbf{c} = (c_1, \cdots, c_N) \in \Re^N$ um vetor unitário ($||\mathbf{c}|| = 1$), com $c_i > 0$, para todo $1 \leqslant i \leqslant N$, e $\mathbf{u} = (u_1, \cdots, u_N) \in \Re^N$. Considere a função $\mathbf{\Phi_c} : \Re^N \to \Re^{2N}$, definida como

$$\mathbf{\Phi_c}(\mathbf{u}) = \Big(c_1 cos\frac{u_1}{c_1}, c_1 sen\frac{u_1}{c_1}, \cdots, c_N cos\frac{u_N}{c_N}, c_N sen\frac{u_N}{c_N}\Big). \tag{5.1}$$

A função $\mathbf{\Phi_c}$ é uma parametrização de um toro planar (em inglês *flat torus*), no qual é um superfície N dimensional contida na esfera unitária $S^{2N-1} \in \Re^{2N}$.

Essa função tem diversas características [64], uma delas é que a distância entre dois pontos do mesmo toro é

$$||\mathbf{\Phi_c}(\mathbf{u}) - \mathbf{\Phi_c}(\mathbf{u'})|| = 2\sqrt{\sum_i c_i^2 sen^2\Big(\frac{u_i - u_i'}{2c_i}\Big)}. \tag{5.2}$$

Criando a possiblidade de dois pontos $\mathbf{u}$ e $\mathbf{u'}$ próximos serem levados a dois pontos $\mathbf{\Phi_c}(\mathbf{u})$ e $\mathbf{\Phi_c}(\mathbf{u'})$ distantes, quando comparados com os primeiros.

Utilizando essa curva, é possível definir o esquema de modulação não linear que será utilizado no protocolo de QKD. Considere $N = 2$, de modo que

$$\mathbf{\Phi_c}(\mathbf{u}) = \Big(c_1 cos\frac{u_1}{c_1}, c_1 sen\frac{u_1}{c_1}, c_2 cos\frac{u_2}{c_2}, c_2 sen\frac{u_2}{c_2}\Big) \tag{5.3}$$

e o segmento de reta $\mathbf{v}(m) = (2\pi u_1 c_1 m, 2\pi u_2 c_2 m)$, $m \in [-1, 1]$, $\sqrt{c_1^2 + c_2^2} = 1$, com $c_1, c_2 > 0$, e $u_1, u_2 \in \mathbb{Z}$. A modulação $\mathbf{s}_{T_c}(x)$ será dada pela composição $\mathbf{\Phi_c}(\mathbf{v})$, ou seja,

$$\mathbf{s}_{T_c}(x) = \Big(c_1 cos(2\pi u_1 m), c_1 sen(2\pi u_1 m), c_2 cos(2\pi u_2 m), c_2 sin(2\pi u_2 m)\Big). \tag{5.4}$$

Essa curva em $\Re^4$ dá u_1 voltas em torno do círculo obtido pela sua projeção nas duas primeiras coordenadas e u_2 voltas em torno do círculo de raio c_2 dado pelas suas duas últimas coordenadas, produzindo o que é chamado de nó do tipo (u_1, u_2) no toro planar $T_\mathbf{c}$. Na Fig. 9 é ilustrado essa curva para $(u_1, u_2) = (4, 5)$, e a sua projeção estereográfica no $\Re^3$.

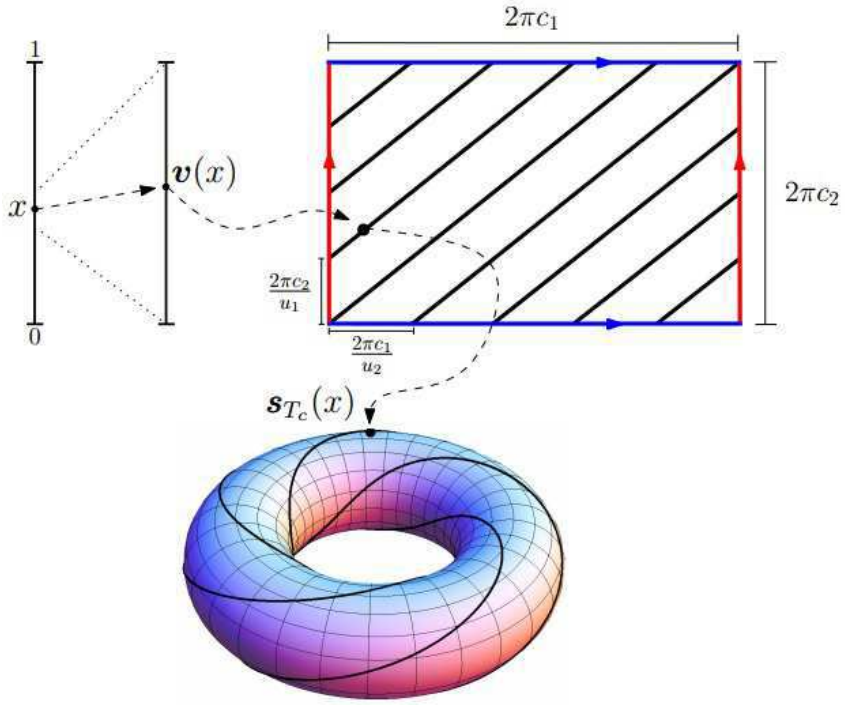

Figura 9 – Processo de codificação.

Na prática, o ponto selecionado no toro planar corresponde aos valores da posição e *momenum* dos dois modos do campo eletromagnético utilizado, ou seja, a primeira e segunda coordenadas de $\mathbf{s}_{T_c}(x)$ são a posição e *momentum* do primeiro modo, enquanto a terceira e quarta coordenadas correspondem às mesmas quantidades físicas, mas agora do segundo modo. Pelo princípio de inderteminação de Heisenberg, a posição medida por Bob desse ponto será descrita por uma distribuição de probabilidade, fato que é descrito na subseção a seguir.

5.3 O Protocolo de Distribuição Quântica de Chave Secreta Proposto

O protocolo proposto é bastante similar com os propostos por Cerf, et al. [33] e o de Grosshans e Grangier [42]. Considere, inicialmente, que Alice pode medir o estado do canal, ou seja, ela consegue ter a informação do nível de ruído do canal quântico que ela irá implementar o QKD e que esse ruído seja igual a η. Os seguintes passos são repetidos em cada rodada (ou *round*) do protocolo de distribuição quântica de chave secreta proposto:

1. Alice gera a mensagem m, que tem distribuição uniforme entre $[-1, 1]$[1] e a ser

[1] Para fontes com outros tipos de distribuição, como gaussiana, é possível o uso de funções compostas, nas quais mapeiam essa distribuição para a distribuição uniforme e limitada ao intervalo fechado que

enviada pelo canal quântico. Com esse valor, ela sabe qual o ponto na modulação que será enviado, ponto que é dado por $\mathbf{s}_{T_c}(x)$;

2. Ela escolhe aleatoriamente em qual das duas direções que ela efetuará a compressão do estado comprimido bimodal, sendo essa direção denotada por i. Para a modulação que é utilizada, as duas possíveis direções são

$$\boldsymbol{Direção}_1 = \mathbf{T} + \mathbf{N} \tag{5.5}$$

$$\boldsymbol{Direção}_2 = \mathbf{T} - \mathbf{N}, \tag{5.6}$$

onde $\mathbf{T}$ e $\mathbf{N}$ são os versores tangente e normal à $\mathbf{s}_{T_c}(m)$, respectivamente, e são iguais a

$$\mathbf{T} = \frac{1}{\sqrt{c_1^2u_1^2 + c_2^2u_2^2}}\Big(\quad -c_1u_1sen(2\pi u_1x), c_1u_1cos(2\pi u_1x), \tag{5.7}$$

$$-c_2u_2sen(2\pi u_2x), c_2u_2cos(2\pi u_2x)\Big), \tag{5.8}$$

$$\mathbf{N} = \frac{1}{\sqrt{c_1^2u_1^4 + c_2^2u_2^4}}\Big(\quad -c_1u_1^2sen(2\pi u_1x), -c_1u_1^2cos(2\pi u_1x), \tag{5.9}$$

$$-c_2u_2^2sen(2\pi u_2x), -c_2u_2^2cos(2\pi u_2x)\Big). \tag{5.10}$$

3. Ela prepara um estado comprimido com compressão na direção que ela sorteou e intensidade dada por r;

4. Posteriormente, Alice escolhe os valores de u_1, u_2, c_1, c_2, observando que u_1 e u_2 fornecem o número de voltas do círculo nas coordenadas, como foi mencionado na subseção anterior, e c_1 e c_2 estão relacionados com as distâncias entre duas partes da curva. Para o caso dessa disertaçao, escolheu-se $u_1 = u_2 = u = 4$ por mera comodidade e

$$c_i = \frac{u}{\pi(V_m + V_i + \chi)} \tag{5.11}$$

$$c_{(i \mod 2)+1} = \sqrt{1 - c_i^2}, \tag{5.12}$$

em que $V_i = sN_0$, com N_0 sendo a variância do estado do vácuo, e $\chi = (1-\eta)/\eta$ é a variância do ruído do canal. Os valores de c_1 e c_2 devem depender do ruído do canal, a escolha feita para o protocolo proposto foi através de análises qualitativas e numéricas, podendo haver outras escolhas mais eficientes.

vai de -1 a 1 [65, 58].

5. Em seguida, ela desloca as quadraturas X_1^1, X_2^1, X_1^2 e X_2^2 (X_i^j é a quadratura i no modo j) do estado comprimido bimodal criado para a posição de modulação $\mathbf{s}_{T_c}(m)$ e envia para Bob, ou seja,

$$(X_1^1, X_2^1, X_1^2, X_2^2) = \mathbf{s}_{T_c}(m). \tag{5.13}$$

Uma noção do estado enviado para Bob pode ser entendida a partir da projeção estereográfica, como é apresentada na Fig.10;

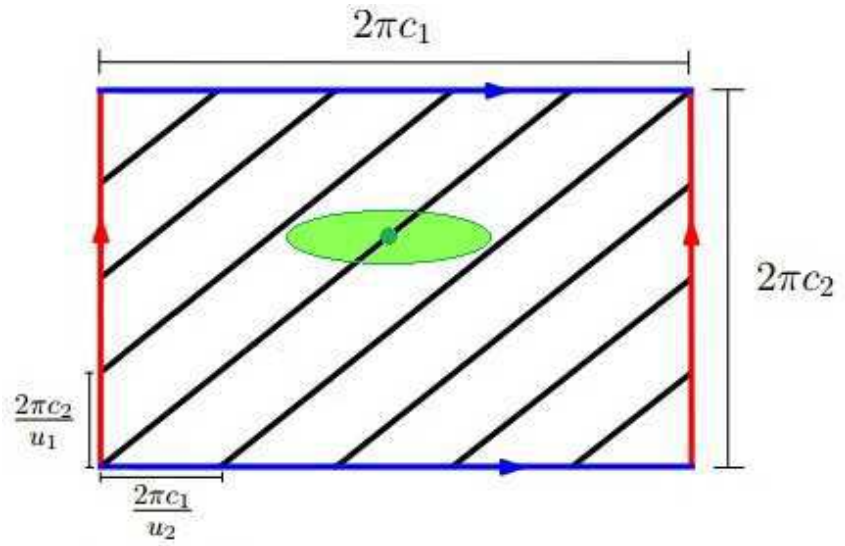

Figura 10 – Visualização da projeção estereográfica do estado enviado por Alice para Bob. O ponto em verde é o estado criado por Alice e a região sombreada em verde corresponde na região onde o estado pode estar, devido ao princípio de indeterminação de Heisenberg.

6. O primeiro passo de Bob é fazer uma demodulação projetiva, de modo que ele faz uma projeção do ponto recebido, que está relacionado com os valores $(X_1^1, X_2^1, X_1^2, X_2^2)$ recebidos por ele, no toro em que a curva de modulação está associada. Isso implica que o ponto que Bob recebe pode ser visto como um ponto no plano bidimensional, veja Fig. 10, com as variâncias que serão descritas nos passos posteriores. Posteriormente, ele escolhe aleatoriamente qual direção medir. Se ele escolher a mesma direção que Alice efetuou a compressão, o protocolo prossegue; caso contrário, ele é reiniciado. Isso é decidido na fase de discussão pública posterior à medida de Bob;

7. Uma vez que Bob mediu a quadratura correta, Alice divulga, através de um canal público e autenticado, duas informações. Primeiramente, os parâmetros da o valor da direção oposta da modulação que Bob não foi capaz de obter. Assim, Bob consegue estimar o valor de m, que será denotado por $\hat{m}_{Bob}$.

Observe que um fato importante desse protocolo é a escolha de c_1 e c_2. O valor de c_i é tal que ele é pequeno da base escolhida, o motivo disso é que a compressão feita sobre estado comprimido ajuda ao ruído do canal ser suprimido nessa direção, o que não ocorre na direção oposta. Por exemplo, se a direção escolhida for a 1, então o valor de c_1 é muito pequeno, equanto a de c_2 é grande. Como o protocolo só prossegue se Bob medir na base correta, então o valor que ele terá de $\hat{m}_{Bob}$ será bastante próximo de m. Isso não ocorre para uma espiã que esteja observando o canal, como será mostrado a seguir com os cálculos da informação mútua.

Com as condições apresentadas, a variância do estado enviado relacionada com a característica quântica do estado comprimido é igual a rN_0 na direção em que Alice escolheu, o que corresponde a uma compressão, e N_0/r na outra, em que N_0 é a variância do estado do vácuo. Também há a variância referente ao canal, se o ruído do canal é χ, então a variância introduzida por esse ruído sobre o estado enviado, que afeta as duas quadraturas de forma similar, é igual a χN_0. Por exemplo, se Alice escolher a direção de compressão como sendo a direção 2, então Bob observará um estado que tem, direção 1, variância igual a $N_0/r + \chi N_0$ e, na direção 2, igual a $rN_0 + \chi N_0$.

É possível pensar na impossibilidade prática de se construir um estado comprimido do jeito que está sendo necessário porém, uma explicação simples pode mostrar que isso é possível. A construção de variáveis aleatórias conjuntamente gaussianas, por exemplo o par (Y, Z), tendo a característica que a sua distribuição possui uma direção em que a variância é reduzida e outra que é aumentada é bastante simples [32]. Para isso, considere que a matriz de covariância das variáveis aleatórias seja $\mathbf{\Sigma}$ assim, os autovetores dessa matriz correspondem à direção em que há o aumento ou diminuição da variância e os seus autovalores à magnitude dessa variância. Consequentemente, se a matriz de covariância do estado comprimido bimodal é $\mathbf{\Sigma}_{bimodal}$, então só é necessário que se construa um estado comprimido que tem uma matriz de covariância com autovetores iguais a $\boldsymbol{Direção}_1$ e a $\boldsymbol{Direção}_2$ e com autovalores rN_0 e N_0/r, para o autovetor correspondendo à direção comprimida e a não comprimida, respectivamente.

Do ponto de vista de comparação entre o protocolo criado e os que foram tomados como base, os propostos por Cerf, et al. [33] e o de Grosshans e Grangier [42], tem-se que a única diferença entre eles é no método de geração do estado quântico. Nos de Cerf e de Grosshans e Grangier, a quadratura do estado enviado é dada pelo valor m gerado por Alice, enquanto que no nosso é feita uma correspondência não linear, dada por $\mathbf{s}_{T_\mathbf{c}}$. Outra diferença é que eles utilizam apenas uma quadratura e na nossa há duas, mesmo assim, a comparação desses protocolos é possível pois o estado comprimido bimodal é emaranhado, de forma que ele é descrito por uma único estado quântico inseparável.

5.4 Resultados Numéricos

Para a análise do protocolo, foi feito a estimativa da informação mútua entre Alice e Bob e entre Alice e Eva por meio do método de Kraskov [66]. Este método estima a informação mútua a partir de amostras da distribuição conjunta das variáveis aleatórias. Eles utilizam a ideia de k vizinhos mais próximos. Com isso, ele sugere um método eficiênte e adaptativo. Infelizmente, não é objetivo desse trabalho o estudo de tal método de estimação de informação mútua, apenas a sua utilização do método é necessária, por isso, para obter mais informação sobre esse método, veja o trabalho de Kraskov [66].

O tipo de ataque que foi considerado para Eva é o seguinte. Se o ruído do canal visto por Bob é dado por χN_0, então Eva efetua o ataque substituindo o meio de transmissão entre Alice e Bob por um sem ruído e coloca, em algum local entre eles, um *beam-splitter* de transmissividade igual a η. Isso faz com que Bob continue visualizando o mesmo ruído referente ao canal, o que mascara a ação da espiã, e Eva observe um ruído igual a $\chi^{-1}N_0$. Durante a transmissão do estado de Alice, Eva pode ou não acertar a base escolhida, mas sempre saberá a informação que Alice envia para Bob durante a parte de comunicação no canal público, ou seja, Eva sabe qual é a curva que gera os valores das quadraturas do estado a ser enviado e qual é o valor da quadratura que Alice informa para Bob.

Para a simulação, foi considerado que $N_0 = 1$, $u_1 = u_2 = u = 4$, c_1 e c_2 são dados pela Eq. 5.12. Como o primeiro procedimento de Bob é fazer uma projeção do ponto recebido no toro em que a curva de modulação está associado, então é possível, para a simulação, considerar que estamos trabalhando em um espaço bidimensional. Dessa forma, a descrição da variável aleatória que Bob recebe é a mesma apresentada na Fig. 10. Por exemplo, considere que $r = 0,5$, $\chi = 0,7$ e que Alice gera o valor $m = 0,2$ e comprime na direção 1. Esse ponto corresponderá ao vetor $(21,6; 13,8857)$ (este valor advêm da atribuição de m na Eq. 5.4) porém, por causa da variância do estado comprimido, ponto que é enviado por Alice $(21,4527; 13,5646)$. Bob recebe $(21,8118; 13,8857)$. Ele calcula qual é o ponto mais próximo da curva, com relação àquele que recebeu, e enconta $(21,75; 13,9821)$. Este ponto leva a $\hat{m}_{Bob} = 0,2031$.

Para Eva, quando ela não acerta a base, o estado recebido é $(23,8409; 13,8857)$, e quando ela acerta é $(23,8409; 15,9528)$. Depois da demodulação, os pontos correspondendo a Eva acertar ou não a base são, respectivamente, $(23,184; 14,904)$ e $(24,0; 15,4286)$. Esses valores resultam em $\hat{m}_{Eva} = 0,2330$ e $\hat{m}_{Eva} = 0,25$. Observe que, mesmo ela visualizando o canal e acertando a base, o seu valor obtido não é mais próximo do valor que Alice gerou quando comparado com o obtido por Bob.

Para um fator de compressão mais usual, $r = 0,5$, os resultados da simulação obtidos são mostrados nas Figs. 11, 12 e 13. Nessas figuras, I_{AB} e I_{AE} são, respectivamente,

as informações mútuas, depois do protocolo, entre Alice e Bob e Alice e Eva. Também é mostrado $I_{AB} - I_{AE}$, que corresponde à informação líquida, ela é a quantidade de informação que realmente pode ser utilizada para construir uma chave quântica secreta. Por esse motivo, ela deve ser positiva, caso contrário Eva possuiria mais informação que Bob, o que impossibilitaria em se construir uma chave secreta. Esses valores são calculados do conjunto de valores de m, $\hat{m}_{Bob}$ e $\hat{m}_{Eva}$ gerados durante a simulação, ou seja, o programa utilizado para calcular a informação mútua pelo método de Kraskov toma como entrada o conjunto de valores de m e $\hat{m}_{Bob}$, fornecendo como saída I_{AB}, e m e $\hat{m}_{Eva}$

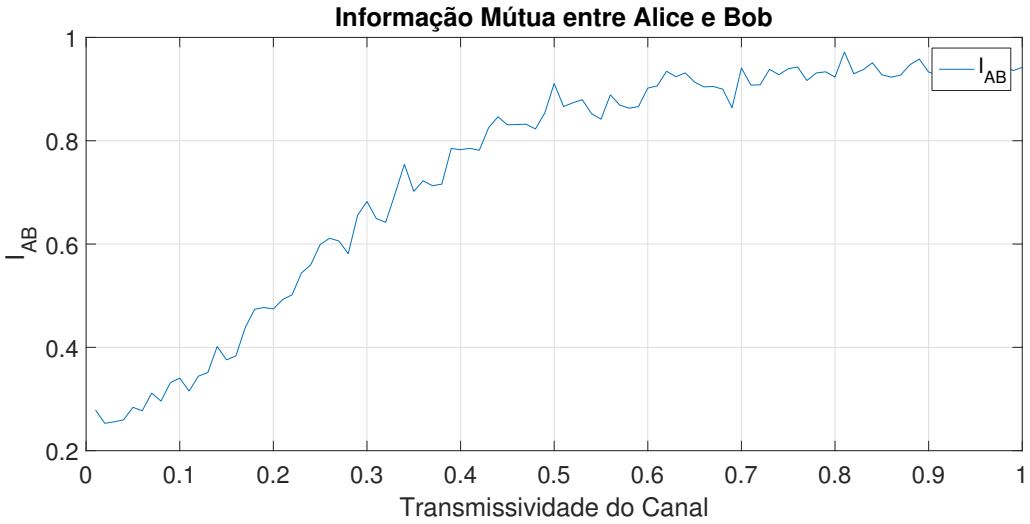

Figura 11 – Informação mútua entre Alice e Bob para $r = 0,5$.

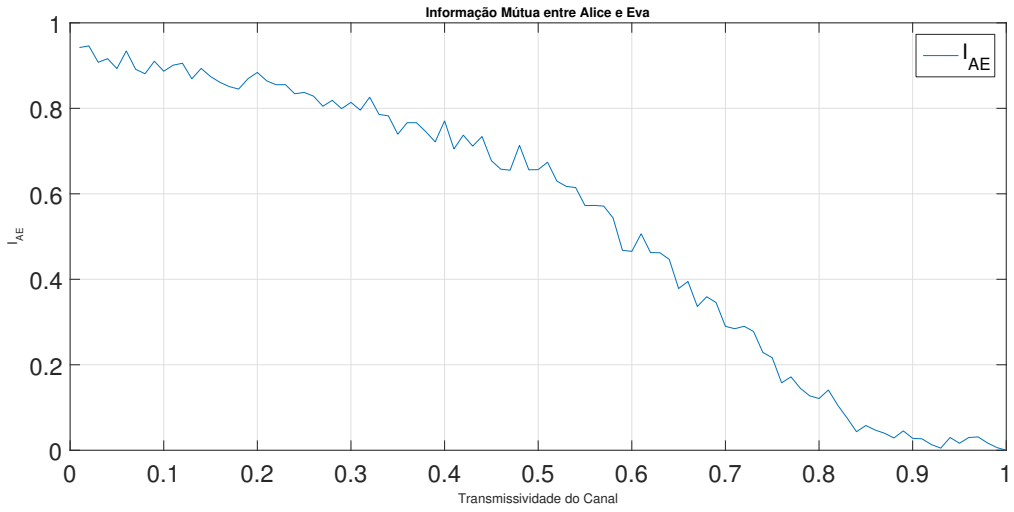

Figura 12 – Informação mútua entre Alice e Eva para $r = 0,5$.

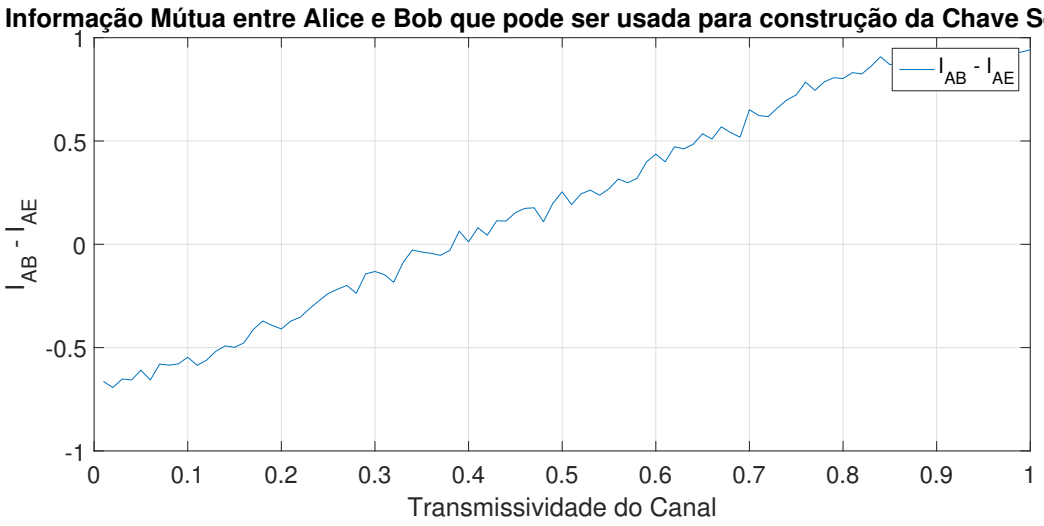

Figura 13 – Informação mútua que pode ser utilizada para se construir a chave secreta, para $r = 0,5$.

Com o parâmetro de compressão que foi utilizado, nota-se que se a transmissividade do canal for maior que $0,4$, é possível gerar uma chave secreta entre Alice e Bob. Se o ambiente de comunicação possui transmissividade menor, o protocolo aqui proposto torna possível, mesmo em tais situações, a geração de chave secreta, apenas com a necessidade de uma maior fator de compressão. Nenhum trabalho anterior, de conhecimento do autor dessa dissertação, possui tal versatilidade. Isso é visto nas figuras a seguir.

Para $r = 0,05$, foi obtido os seguintes resultados apresentados nas Figs. 14-16.

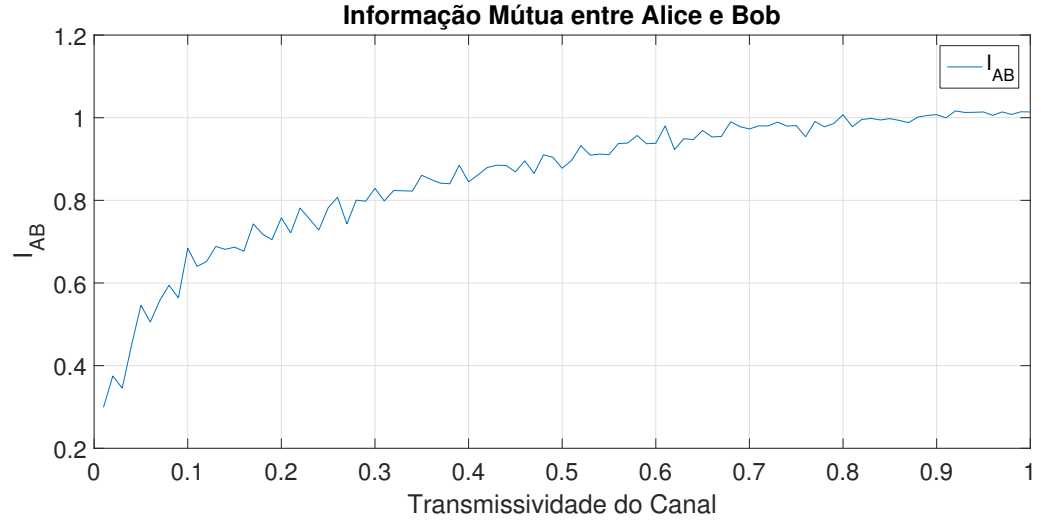

Figura 14 – Informação mútua entre Alice e Bob para $r = 0,05$.

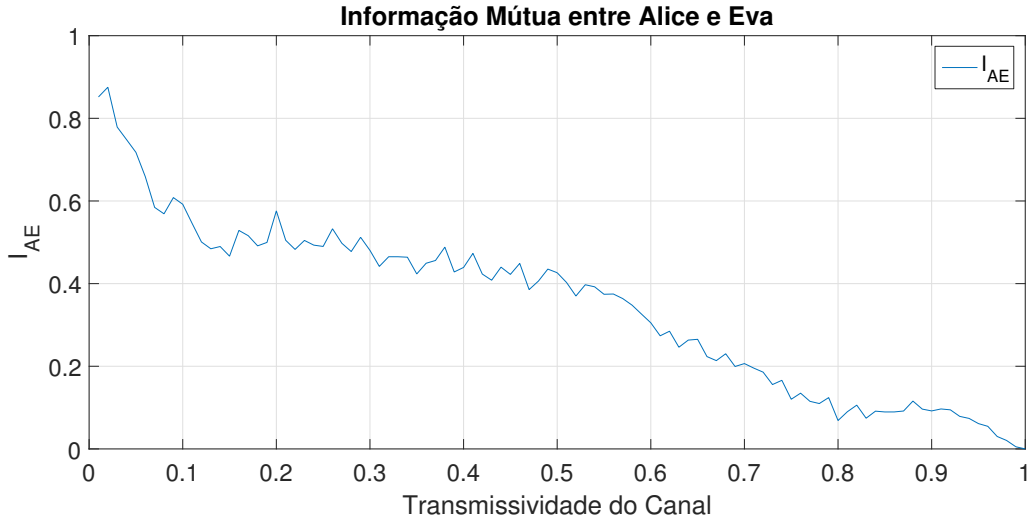

Figura 15 – Informação mútua entre Alice e Eva para $r = 0,05$.

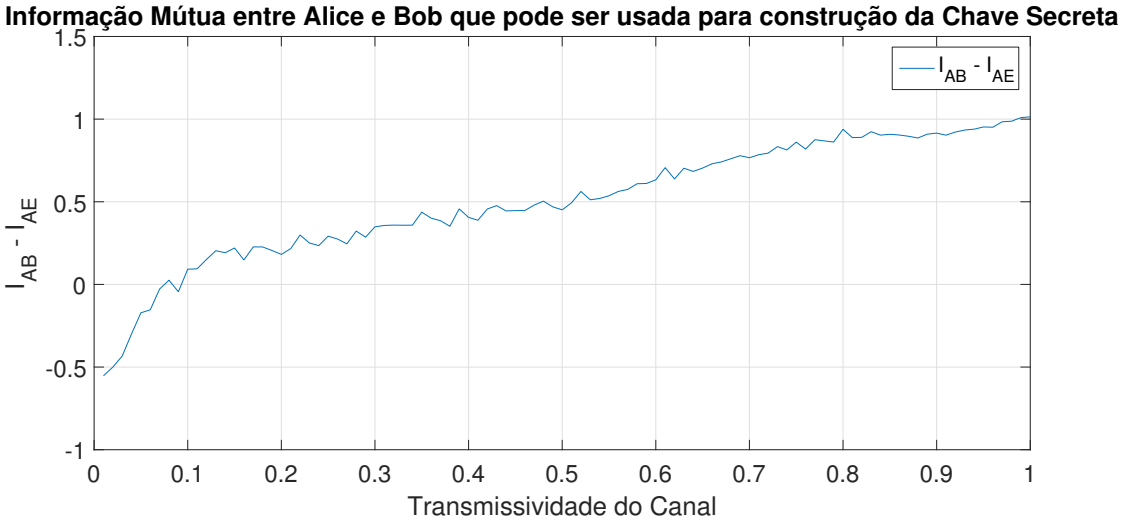

Figura 16 – Informação mútua que pode ser utilizada para se construir a chave secreta, para $r = 0,05$.

Utilizando esses novos parâmetros, é possível construir uma chave secreta mesmo se a transmissividade do canal esteja entre $0,1$ e $0,5$. Comparando com outros resultados [33, 42, 17], onde há a necessidade da transmissividade do canal seja maior que $0,5$, quando considerado o mesmo tipo de ataque, é notado que o protocolo aqui proposto possui uma vantagem fundamental. Ele fornece um método de superar essa barreira que há nos protocolos já existentes. Observe que todos os resultados aqui apresentados são para ataques do tipo *beam-splitter*. Assim, talvez para outros tipos de ataques o protocolo não seja eficiente, caso que ainda será analizado em pesquisas futuras

6 Considerações Finais

Neste capítulo, são apresentadas as considerações finais do trabalho. Nas seções seguintes é apresentada uma síntese do trabalho desenvolvido, algumas considerações importantes, tais como vantagens e limitações dos métodos desenvolvidos e elencadas possíveis atividades futuras para continuação do trabalho.

6.1 Conclusões

Neste trabalho foi proposta e numericamente avaliada a utilização de esquemas de modulação não lineares, tradicionalmente definidos no contexto da Engenharia de Telecomunicações, para a preparação de estados quânticos de variáveis contínuas em um sistema de distribuição quântica de chaves. Essas contribuições utilizaram as teorias de comunicação não lineares e de variáveis contínuas em mecânica quântica para dar síntese ao protocolo proposto e analisado. No protocolo proposto pode-se notar três características fundamentais: i) Utiliza elementos fundamentais para a sua implementação, tais como elementos ópticos; ii) O protocolo apresentado permite adaptação em função do nível de ruído; iii) Fornece alta quantidade de informação para ser utilizada na construção da chave secreta. Todas as análises foram feitas por meio de simulações e os resultados serviram para validar o protocolo desenvolvido.

6.2 Continuação da pesquisa

Uma lista de possíveis trabalhos futuros, dando continuidade ou utilizando o presente trabalho, é apresentada a seguir:

- Implementação física e teste do protocolo que foi construído através de sistemas de fibra óptica e geração não linear de estados comprimidos;
- Descrição matemática do aparato de medida utilizado na parte de detecção de Bob;
- Análise do protocolo sobre outros possíveis ataques de espião, tal como o ataque coletivo.

Referências

1 FERGUSON, N.; SCHNEIER, B.; KOHNO, T. *Cryptography Engineering: Design Principles and Practical Applications*. [S.l.]: Wiley, 2010. Citado 4 vezes nas páginas 15, 16, 44 e 45.

2 KATZ, J.; LINDELL, Y. *Introduction to Modern Cryptography*. [S.l.]: Chapman and Hall/CRC, 2014. Citado 2 vezes nas páginas 15 e 44.

3 PAAR, C.; PELZL, J.; PRENEEL, B. *Understanding Cryptography: A Textbook for Students and Practitioners*. [S.l.]: Springer, 2010. Citado 6 vezes nas páginas 15, 16, 17, 44, 45 e 51.

4 KAHN, D. *The Codebreakers: The story of secret writing*. [S.l.]: Macmillan, 1996. Citado na página 15.

5 Gilbert S. Vernam. *Secret Signaling System*. 1918, US1310719 A. Citado na página 15.

6 REJEWSKI, M. An application of the theory of permutations in breaking the enigma cipher. *Applicationes mathematicae*, 1980. Citado na página 15.

7 SHANNON, C. E. Communication theory of secrecy systems. *Bell System Tech. Journal*, 1949. Citado 2 vezes nas páginas 15 e 46.

8 DIFFIE, W.; HELLMAN, M. Multi-user cryptographic techniques. *AFIPS Proceedings*, 1976. Citado na página 15.

9 ASSCHE, G. van. *Quantum Cryptography and Secret-Key Distillation*. [S.l.]: Cambridge University Press, 2012. Citado 2 vezes nas páginas 16 e 52.

10 GISIN, N.; RIBORDY, G.; TITTEL, W.; ZBINDEN, H. Quantum cryptography. *Rev. Mod. Phys.*, 2002. Citado 4 vezes nas páginas 16, 17, 51 e 53.

11 BENNETT, C. H.; BRASSARD, G. Quantum cryptography: Public key distribution and coin tossing. In: *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*. [S.l.: s.n.], 1984. Citado 4 vezes nas páginas 16, 47, 48 e 49.

12 OESTERLING, L.; HAYFORD, D.; FRIEND, G. Comparison of commercial and next generation quantum key distribution: Technologies for secure communication of information. In: *2012 IEEE Conference on Technologies for Homeland Security (HST)*. [S.l.: s.n.], 2012. Citado na página 16.

13 FOX, M. *Quantum Optics: An Introduction*. [S.l.]: Oxford University Press, 2006. Citado 2 vezes nas páginas 16 e 27.

14 LOOCK, S. L. B. P. van. Quantum information with continuous variables. *Rev. Mod. Phys.*, American Physical Society, v. 77, p. 513–577, Jun 2005. Disponível em: <http://link.aps.org/doi/10.1103/RevModPhys.77.513>. Citado na página 16.

15 SCARANI, V.; BECHMANN-PASQUINUCCI, H.; CERF, N. J.; DUSEK, M.; LUTKENHAUS, N.; PEEV, M. The security of practical quantum key distribution. *Rev. Mod. Phys.*, American Physical Society, v. 81, p. 1301–1350, Sep 2009. Disponível em: <http://link.aps.org/doi/10.1103/RevModPhys.81.1301>. Citado na página 16.

16 WOZENCRAFT, J. M.; JACOBS, I. M. *Principles of Communication Engineering*. [S.l.]: Waveland Pr. Inc., 1990. Citado 4 vezes nas páginas 16, 59, 65 e 66.

17 GROSSHANS, F.; ASSCHE, G. V.; WENGER, J.; BROURI, R.; CERF, N. J.; GRANGIER, P. Quantum key distribution using gaussian-modulated coherent states. *Nature*, 2003. Citado 2 vezes nas páginas 16 e 79.

18 WEEDBROOK, C.; LANCE, A. M.; BOWEN, W. P.; SYMUL, T.; RALPH, T. C.; LAM, P. K. Quantum cryptography without switching. *Phys. Rev. Lett.*, American Physical Society, v. 93, p. 170504, Oct 2004. Disponível em: <http://link.aps.org/doi/10.1103/PhysRevLett.93.170504>. Citado na página 16.

19 PEREIRA, F. R. F.; NASCIMENTO, E. J. do; ASSIS, F. M. de. Distribuição quântica de chave utilizando modulação não linear. In: *Anais do XXXIII Simpósio Brasileiro de Telecomunicações*. [S.l.: s.n.], 2015. Citado na página 18.

20 PEREIRA, F. R. F.; GUEDES, E. B.; ASSIS, F. M. de. Protocolo para autenticação quântica de mensagens clássicas utilizando variáveis contínuas. In: *Anais do XXXIII Simpósio Brasileiro de Telecomunicações*. [S.l.: s.n.], 2015. Citado na página 18.

21 PEREIRA, F. R. F.; ASSIS, F. M. de. Modulação não-linear de estados coerentes. In: *V Workshop-Escola em Computação e Informação Quântica*. [S.l.: s.n.], 2015. Citado na página 18.

22 NIELSEN, M. A.; CHUANG, I. L. *Quantum Computation and Quantum Information*. [S.l.]: Cambridge University Press, 2011. Citado 9 vezes nas páginas 19, 22, 26, 36, 46, 47, 49, 50 e 51.

23 HEISENBERG, W. Über den anschaulichen inhalt der quantentheoretischen kinematik und mechanik. *Zeitschrift für Physik*, 1927. Citado na página 21.

24 SAKURAI, J. J.; NAPOLITANO, J. J. *Modern Quantum Mechanics*. [S.l.]: Addison-Wesley; 2 edition, 2010. Citado 8 vezes nas páginas 21, 22, 23, 24, 26, 28, 46 e 49.

25 ROBERTSON, H. P. The uncertainty principle. *Phys. Rev.*, 1929. Citado na página 21.

26 GERRY, C.; KNIGHT, P. *Introductory Quantum Optics*. [S.l.]: Cambridge University Press, 2004. Citado 4 vezes nas páginas 27, 31, 37 e 41.

27 GRIFFITHS, D. J. *Introduction to Electrodynamics*. [S.l.]: Addison-Wesley, 2012. Citado na página 27.

28 JACKSON, J. D. *Classical Electrodynamics*. [S.l.]: Wiley, 1998. Citado na página 27.

29 REIF, F. *Fundamentals of Statistical and Thermal Physics*. [S.l.]: Waveland Pr. Inc., 2008. Citado na página 29.

30 FERRARO, A.; OLIVARES, S.; PARIS, M. G. A. Gaussian states in continuous variable quantum information. *ArXiv*, 2004. Citado na página 36.

31 WEEDBROOK, C.; PIRANDOLA, S.; GARCíA-PATRóN, R.; CERF, N. J.; RALPH, T. C.; SHAPIRO, J. H.; LLOYD, S. Gaussian quantum information. *Rev. Mod. Phys.*, 2012. Citado na página 42.

32 JOHNSON, R. A.; WICHERN, D. W. *Applied Multivariate Statistical Analysis*. [S.l.]: Pearson, 2007. Citado 2 vezes nas páginas 43 e 75.

33 CERF, N. J.; LEVY, M.; ASSCHE, G. V. Quantum distribution of gaussian keys using squeezed states. *Phys. Rev. A*, 2001. Citado 7 vezes nas páginas 43, 48, 55, 57, 72, 75 e 79.

34 VERNAM, G. S. Cipher printing telegraph systems for secret wire and radio telegraphic communications. *Journal of the IEEE*, 1926. Citado na página 46.

35 FRALEIGH, J. B. *First Course in Abstract Algebra*. [S.l.]: Pearson, 2002. Citado na página 46.

36 PERES, A. *Quantum Theory: Concepts and Methods*. [S.l.]: Springer, 1993. Citado 2 vezes nas páginas 46 e 47.

37 EKERT, A. K. Quantum cryptography based on bell's theorem. *Phys. Rev. Lett.*, 1991. Citado 2 vezes nas páginas 47 e 48.

38 EINSTEIN, A.; PODOLSKY, B.; ROSEN, N. Can quantum-mechanical description of physical reality be considered complete? *Phys. Rev.*, 1935. Citado na página 47.

39 SERNA, E. H. Quantum key distribution from a random seed. *ArXiv*, 2013. Citado 2 vezes nas páginas 47 e 48.

40 BENNETT, C. H.; BESSETTE, F.; BRASSARD, G.; SALVAIL, L.; SMOLIN, J. Experimental quantum cryptography. *Journal of Cryptology*, 1992. Citado 3 vezes nas páginas 48, 51 e 53.

41 BECHMANN-PASQUINUCCI, H.; GISIN, N. Incoherent and coherent eavesdropping in the six-state protocol of quantum cryptography. *Phys. Rev. A*, 1999. Citado na página 48.

42 GROSSHANS, F.; GRANGIER, P. Continuous variable quantum cryptography using coherent states. *Phys. Rev. Lett.*, 2002. Citado 5 vezes nas páginas 48, 57, 72, 75 e 79.

43 BRASSARD, G.; LüTKENHAUS, N.; MOR, T.; SANDERS, B. C. Limitations on practical quantum cryptography. *Physical Review Letters*, 2000. Citado na página 48.

44 INOUE, K.; WAKS, E.; YAMAMOTO, Y. Differential-phase-shift quantum key distribution using coherent light. *Phys. Rev. A*, 2003. Citado na página 48.

45 WAKS, E.; TAKESUE, H.; YAMAMOTO, Y. Security of differential-phase-shift quantum key distribution against individual attacks. *Phys. Rev. A*, 2006. Citado na página 48.

46 SCARANI, V.; ACíN, A.; RIBORDY, G.; GISIN, N. Quantum cryptography protocols robust against photon number splitting attacks for weak laser pulse implementations. *Phys. Rev. Lett.*, 2004. Citado na página 48.

47 GISIN, N.; RIBORDY, G.; ZBINDEN, H.; STUCKI, D.; BRUNNER, N.; SCARANI, V. Towards practical and fast quantum cryptography. *ArXiv*, 2004. Citado na página 48.

48 STUCKI, D.; BRUNNER, N.; GISIN, N.; SCARANI, V.; ZBINDEN, H. Fast and simple one-way quantum key distribution. *Applied Physics Letters*, 2005. Citado na página 48.

49 KHAN, M. M.; MURPHY, M.; BEIGE, A. High error-rate quantum key distribution for long-distance communication. *New Journal of Physics*, 2009. Citado na página 48.

50 SERNA, E. H. Quantum key distribution protocol with private-public key. *ArXiv*, 2012. Citado na página 48.

51 JOUGUET, P.; ELKOUSS, D.; KUNZ-JACQUES, S. High-bit-rate continuous-variable quantum key distribution. *Phys. Rev. A*, 2014. Citado na página 48.

52 MA, H.-Q.; ZHAO, J.-L.; WU, L.-A. Quantum key distribution based on phase encoding and polarization measurement. *Optics Letters*, 2007. Citado na página 49.

53 SHOR, P. W.; PRESKILL, J. Simple proof of security of the bb84 quantum key distribution protocol. *Phys. Rev. Lett.*, 2000. Citado na página 49.

54 BENNETT, C. H.; BRASSARD, G.; ROBERT, J.-M. Privacy amplification by public discussion. *SIAM J. Comput.*, 1988. Citado na página 53.

55 WEGMAN, M. N.; CARTER, J. L. New hash functions and their use in authentication and set equality. *Journal of Computer and System Sciences*, 1981. Citado na página 53.

56 SHANNON, C. E. Communication in the presence of noise. *Proceedings of the IRE*, 1949. Citado na página 70.

57 KOTEL'NIKOV, V. *The theory of optimum noise immunity*. Tese (Doutorado) — New York: McGraw-Hill, 1959. Citado na página 70.

58 VAISHAMPAYAN, V. A.; COSTA, S. I. R. Curves on a sphere, shift-map dynamics, and error control for continuous alphabet sources. *IEEE Trans. Information Theory*, 2003. Citado 2 vezes nas páginas 70 e 73.

59 CAVALCANTE, R. G.; JR., R. P. Análise da curvatura de modulações não-lineares associadas a curvas. *XXVI SIMPÓSIO BRASILEIRO DE TELECOMUNICAÇÕES*, 2008. Citado na página 70.

60 RAMSTAD, T.; AKYOL, E.; ROSE, K. Optimized analog mappings for distributed source-channel coding. *IEEE Data Compression Conf.*, 2010. Citado na página 70.

61 CAMPELLO, A.; TOREZZAN, C.; COSTA, S. I. R. Curves on flat tori and analog source-channel codes. *IEEE Trans. Information Theory*, 2013. Citado na página 70.

62 ALMEIDA, J.; TOREZZAN, C.; BARROS, J. Spherical codes for the gaussian wiretap channel with continuous input alphabets. *IEEE 14th Workshop on Signal Processing Advances in Wireless Communications (SPAWC)*, 2013. Citado na página 70.

63 GARCIA-FRIAS, J.; HU, Y.; LAMARCA, M. Analog joint source-channel coding using non-linear curves and mmse decoding. *IEEE Transactions on Communications*, 2011. Citado na página 70.

64 JUNIOR, A. C. de A. C. *Reticulados, Projeções e Aplicações à Teoria da Informação*. Tese (Doutorado) — UNICAMP, 2014. Citado 2 vezes nas páginas 70 e 71.

65 SAKRISON, D. J. *Notes on Analog Communication*. [S.l.]: New York: Van Nostrand Reinhold, 1970. Citado na página 73.

66 KRASKOV, A.; STöGBAUER, H.; GRASSBERGER, P. Estimating mutual information. *Phys. Rev. E*, 2004. Citado na página 76.