UNIVERSIDADE ESTADUAL DE CAMPINAS

INSTITUTO DE FÍSICA GLEB WATAGHIN - IFGW

DOUGLAS DELGADO DE SOUZA

CRIPTOGRAFIA QUÂNTICA COM ESTADOS COMPRIMIDOS DA LUZ

DISSERTAÇÃO DE MESTRADO APRESENTADA AO
INSTITUTO DE FÍSICA GLEB WATAGHIN DA UNICAMP
PARA OBTENÇÃO DO TÍTULO DE MESTRE EM FÍSICA.

ORIENTADOR

PROF. DR. ANTONIO VIDIELLA BARRANCO

ESTE EXEMPLAR CORRESPONDE À VERSÃO FINAL DA DISSERTAÇÃO
DEFENDIDA PELO ALUNO, E ORIENTADA PELO PROF. DR.

Antonio Vidiella Barranco

CAMPINAS, 2011

FICHA CATALOGRÁFICA ELABORADA PELA BIBLIOTECA DO IFGW - UNICAMP

So89c

Souza, Douglas Delgado de
Criptografia quântica com estados comprimidos da luz / Douglas Delgado de Souza. – Campinas, SP: [s.n.], 2011.

Orientador: Antonio Vidiella Barranco.
Dissertação (mestrado) - Universidade Estadual de Campinas, Instituto de Física "Gleb Wataghin".

1. Criptografia. 2. Informação quântica. 3. Criptografia quântica. 4. Distribuição quântica de chaves. I. Vidiella Barranco, Antonio. II. Universidade Estadual de Campinas. Instituto de Física "Gleb Wataghin". III. Título.

(smcc/ifgw)

- **Título em inglês:** Quantum cryptography with squeezed coherent states of light
- **Palavras-chave em inglês (Keywords):**
  1. Cryptography
  2. Quantum infomation
  3. Quantum cryptography
  4. Quantum key distribution
- **Área de concentração:** Física Geral
- **Titulação:** Mestre em Física
- **Banca examinadora:**
  Prof.Antonio Vidiella Barranco
  Prof. Salomon Sylvain Mizrahi
  Prof. Marcos Cesar de Oliveira
- **Data da defesa:** 06-04-2011
- **Programa de Pós-Graduação em:** Física

MEMBROS DA COMISSÃO JULGADORA DA TESE DE MESTRADO DE **DOUGLAS DELGADO DE SOUZA 088963** APRESENTADA E APROVADA AO INSTITUTO DE FÍSICA "GLEB WATAGHIN", DA UNIVERSIDADE ESTADUAL DE CAMPINAS, EM 06 / 04 / 2011.

COMISSÃO JULGADORA:

Prof. Dr. Antonio Vidiella Barranco - Orientador do Candidato
DEQ/IFGW/UNICAMP

Prof. Dr. Salomon Sylvain Mizrahi – DF/UFSCar

Prof. Dr. Marcos Cesar de Oliveira – DFMC/IFGW/UNICAMP

Agradecimentos

Gostaria de agradecer à minha família e a todos os meus amigos e professores de graduação e pós, por esta longa jornada de estudos, pelo apoio, pelas idéias e por fazerem a minha vida mais feliz e completa. Citemos alguns deles: gostaria de agradecer

Aos meus pais, Marcolino Pereira de Souza e Esmiriam Leme Delgado Pereira de Souza, pela dedicação em me ensinarem o que é certo e me darem o exemplo máximo de dignidade, correteza, força e coragem;

Aos meus irmãos, Cézar Delgado de Souza, Estela Delgado de Souza e Selma Delgado de Souza Moro, todos mais velhos, por me abrirem os caminhos e os olhos, me preparando para as dificuldades da vida;

Ao meu amigo e orientador Antonio Vidiella Barranco, por ter me acolhido e decidido se aventurar com maestria nesta área de criptografia quântica, indicando sempre o melhor caminho;

Aos amigos Michael Jonathan Franco de Oliveira e Michael Willian de Castro Gomes pela nossas trapalhadas na adolescência e frutífera relação neste início de vida adulta;

Aos amigos Pablo Ferreira de Souza e Aline Ramires Neves de Oliveira, com quem pude enxergar mais longe e aprimorar meu gosto pela vida e pela física;

Aos amigos Márcio Rodrigues Soares, Fernando dos Santos Dutra, Dorival Pereira dos Santos Júnior e Isaías Alves da Silva e às amigas Michele Cristina Pedroso, Renata Kazumi Takaesu, Cristiane de Oliveira Barbosa, Graziani Ferrer Corrêa, Graziela Ferrer Corrêa, Juliana Aparecida dos Santos Chaves, Regiane da Silveira, Thaís Nascimento França, Maiza Lopes de Carvalho e Terezinha Gagliardi, pela nossa maravilhosa e contínua convivência. Nós fizemos da UFSCar mais do que nossa casa, temos lá um lugar especial de lembranças alegres e doces. Ainda hoje, lá é o meu local preferido para descanso, quando posso reencontrar alguns destes meus amigos e respirar aquele ar puro e fresco.

Quando cheguei na UNICAMP, recebi de presente novos amigos: gostaria de agradecer a Gustavo Lázero Deçordi, Cesar José Calderon Filho e Julio Cesar González Henao pela nossa atual convivência, troca de idéias e por me ajudarem sempre que preciso.

Com estas pessoas eu conheci a importância do respeito, as vantagens da convivência, a irrelevância da timidez e a força da amizade.

Por fim, gostaria de agradecer a todos que garantem a excelência do Instituto de Física "Gleb Wataghin" e ao Conselho Nacional de Desenvolvimento Científico e Tecnológico (CNPq), pelo apoio financeiro aos meus estudos do mestrado e também da iniciação científica.

"A vida é a arte do encontro, embora haja tanto desencontro pela vida."

Vinícius de Moraes

Resumo

Neste trabalho, introduzimos um protocolo para a distribuição quântica de chaves (QKD) que faz uso de três estados comprimidos da luz: dois estados de bit, utilizados para a transmissão de informação, e um estado de Isca, utilizado para a detecção de espionagem. Seu desenvolvimento teve como base o protocolo de P. Horak (H04) para estados comprimidos, que por sua vez consiste de uma generalização do protocolo de R. Namiki e T. Hirano (NH03) para estados coerentes. Analisamos sua segurança considerando dois tipos de ataques: ataque por medida simultânea das quadraturas e ataque por troca do canal por canal superior. Para esta análise utilizamos uma descrição em termos da função de Wigner, obtendo a partir dela distribuições de probabilidade conjuntas e marginais. Da distribuição para os estados de Isca definimos uma *Medida da Espionagem* M, e discutimos sua utilidade para o cálculo da taxa de informação vazada para Eva em cada ataque. Por fim, para o ataque por troca do canal, analisamos o efeito da introdução de um limiar de pós-seleção sobre as informações de Bob e Eva, demonstrando que maiores distâncias de transmissão (menores transmissividades) podem ser suportadas pelo protocolo com o aumento deste parâmetro, ao custo de menores taxas de aceitação de bits.

Abstract

In this work, we introduce a new protocol for Quantum Key Distribution which makes use of three squeezed coherent states of light: two bit states, used for transmission of information, and a Decoy state, used for eavesdropping detection. Its development was based on the protocol for squeezed coherent states suggested by P. Horak [39], which in turn consists of a generalization of the protocol by R. Namiki and T. Hirano [38] for coherent states. We analyze its security by considering two kinds of attack: simultaneous quadrature measurement attack and superior channel attack. For this analysis we use a description in terms of the Wigner function, obtaining from it some joint and marginal probability distributions. From the distribution for the Decoy states we define an *Eavesdropping Measure* M, and discuss its usefulness in calculating the rate of information leaked to Eve in each attack. Finally, for the superior channel attack, we analyze the influence of a post-selection threshold over the Bob and Eve information, showing that, by raising this parameter, larger transmission distances (smaller transmittivities) can be handled by the protocol at the expense of lower bit acceptance rates.

Apresentação

Este trabalho encontra-se dividido em três partes:

Na primeira parte, Capítulo 1, é apresentada a importância da criptografia e diversos conceitos fundamentais são introduzidos através de uma abordagem histórica. No Capítulo 2 são delineados alguns tipos de algoritmos de criptografia atuais, que serão úteis na compreensão dos protocolos de criptografia quântica. Ao fim da primeira parte é justificada a necessidade da criptografia quântica em nossa sociedade de plenos avanços tecnológicos.

A segunda parte foi planejada como um preâmbulo. Nela introduzimos todo o ferramental teórico matemático, físico e tecnológico requerido para uma correta manipulação dos protocolos apresentados na terceira parte. Em especial, no Capítulo 6, é apresentada a função de Wigner, cuja aplicação em protocolos de criptografia é um pouco inusitado. Este uso foi descoberto através do *paper* de Horak [39] e mostrou-se bastante atraente para uma análise mais simplificada dos protocolos de variáveis contínuas, sendo portanto adotado neste texto.

Na terceira parte, Capítulo 8, são descritos os primeiros passos da criptografia quântica e dois protocolos fundamentais, que não fazem uso de emaranhamento, são apresentados. Ainda neste capítulo são discutidos cinco tipos de ataques comuns aos sistemas criptográficos quânticos e algumas soluções possíveis. A seguir partimos para os protocolos com variáveis contínuas e codificação discreta, iniciando com um protocolo que faz uso de estados coerentes da luz (Namiki e Hirano 03). Apresentamos o protocolo proposto pelo autor já referido (Horak 04), que faz uso de estados comprimidos, e seguimos seus passos na análise através do uso da função de Wigner. Por fim, no Capítulo 10, propomos um novo protocolo com estados comprimidos e sua segurança é analisada para dois tipos de ataques.

Um dos objetivos deste texto é ser uma literatura especializada, mas completa, simples e agradável, de forma a ser apreciado tanto por *experts* quanto por iniciantes na área de criptografia. As notas de rodapé são trechos explicativos ou fatos curiosos da história da criptografia e ciências relacionadas. Ao final deste trabalho acrescentamos uma pequena lista de sites e multimídias interessantes.

Sumário

Lista de Figuras

Parte I

Criptografia Nossa de Cada Dia

Capítulo 1

Introdução e História

Criptografia (do grego *kryptós*, "escondido", e *gráphein*, "escrita") é o estudo de técnicas que permitem a escrita de mensagens que apenas o destinatário e o remetente conseguem ler. *Criptanálise* (*análysis*, "decomposição") é o estudo de técnicas capazes de revelar o *texto claro* contido nas *mensagens cifradas*[1] sem o conhecimento da *chave* ou do *mecanismo* usado para cifrá-la. A *criptologia* é a ciência que reúne estas duas áreas e algumas outras relacionadas à transmissão secreta de informações, como a esteganografia (*steganos*, "coberto"), onde a mensagem é escrita sem alterações mas apenas o destinatário sabe onde procurá-la (tatuagem no couro cabeludo de escravos, caixotes escritos internamente e cheios de cera, etc), e a criptolalia (*lalos*, "fala"), cujo exemplo mais simples é a "língua do pê" [1, 43].

A criptografia é o produto do trabalho humano em busca de liberdade, privacidade, segurança e soberania de sua nação. A história da humanidade é repleta de conflitos e guerras, seja entre comunidades vizinhas ou países diametralmente opostos na terra. A pressão destas guerras gerou o sumo necessário para nutrir os grandes desenvolvimentos científicos e tecnológicos ocorridos. Nas últimas duas décadas vimos o surgimento e expansão da internet, que conectou as pessoas e transformou o mundo em uma “grande aldeia global”. Experimentamos a extensão de nossas vidas reais para um mundo virtual onde recebemos um endereço e encontramos amigos, nos divertimos, compramos, reivindicamos, discutimos, trabalhamos e divulgamos nosso trabalho. Porém, nossa vida real esteve sempre sujeita a ações criminosas e isto não é diferente no mundo virtual. Lá, temos nossas identidades protegidas por avançados sistemas criptográficos computacionais que garantem nossa privacidade, protegem nossas contas bancárias e autenticam todas as nossas ações. Mas até que ponto ou até quando poderemos depositar nossa confiança nestes sistemas?

Os sistemas criptográficos atuais mais versáteis são baseados nas propriedades matemá-

[1]Cifra é o processo pelo qual o texto claro é convertido em *criptograma* ou *texto cifrado*. Texto claro é a mensagem ainda não processada pela cifra.

ticas de funções de via única. Tais sistemas se aproveitam da *capacidade computacional limitada* de qualquer *possível* espião para gerar tempos médios de criptanálise muitas vezes superiores à idade do universo. O ato de criptanálise torna-se impraticável com a tecnologia disponível à época e isto dá origem à chamada *Segurança Computacional Prática*. Esta segurança é, portanto, temporária e não permite, por exemplo, a ocultação de documentos ou mensagens por um tempo ilimitado.

Hoje o sistema criptográfico mais usado é o RSA[2]. A função de via única usada pelo RSA é a operação de multiplicação de dois números primos muito grandes. Embora um computador pessoal realize este produto sem dificuldades, o processo inverso, de fatoração do resultado em dois números primos, é uma tarefa formidável até para os mais potentes *mainframes* disponíveis atualmente. A dificuldade desta fatoração não é uma propriedade matemática e pode até mesmo, a qualquer momento, ser desmantelada pela descoberta de alguma nova propriedade dos números primos e seu produto, se é que isso já não tenha sido feito secretamente. Desta forma, *aparentemente*, o RSA é praticamente seguro, mas ainda assim é uma solução temporária, pois mesmo que tal propriedade nunca seja descoberta, a evolução tecnológica está nos apresentando gradualmente um novo paradigma da computação, a computação quântica, que nos promete computadores com algoritmos extremamente eficazes na paralelização e fatoração de grandes números. É como preparação para este novo cenário que temos o imprescindível desenvolvimento da *Criptografia Quântica* (QC) e, mais especificamente, da *Distribuição Quântica de Chaves* (QKD).

A *segurança incondicional* da Criptografia Quântica será a solução requerida para o progresso das telecomunicações e internet, mas é também uma busca humana com quase 4000 anos de história [1, 2, 3, 32, 4].

1.1 A batalha *criptografia*×*criptanálise*

Todo grande criptanalista foi um grande criptógrafo. A experiência adquirida na busca de fragilidades em uma cifra dão ao criptólogo condições de criar sua própria cifra, mais simples, mais rápida e imune aos ataques já conhecidos. Isto é o que garante o desenvolvimento da criptologia.

O primeiro registro histórico de algo que poderia ser classificado como criptografia ocorreu em 1900 a.C. no Egito, na tumba de Knumhotep II, onde alguns dos hieróglifos foram trocados por outros "mais importantes e bonitos". Embora esta troca provavelmente não tivesse objetivos criptográficos à época, esta seria a técnica base das *cifras de substituição*

[2]De fato, acredita-se que o protocolo RSA compõe o software com mais cópias distribuídas do planeta, mais do que o Microsoft Windows® ou Internet Explorer® [2].

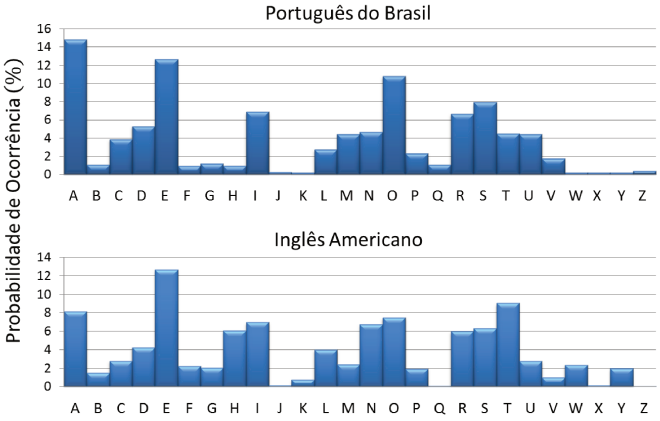


Figura 1.1: Comparação da frequência de ocorrência de letras no Português do Brasil e no Inglês Americano [43], dada em porcentagem.

desenvolvidas posteriormente, como o *Código de Políbio*, a *Cifra de César*[3] e muitas outras.

1.2 Análise de frequências

Durante o período medieval de nossa história o oriente abrigou os desenvolvimentos ocorridos na criptologia. Alguns livros foram publicados e o famoso Kama Sutra, de Vatsyayana, incluía duas técnicas criptográficas dentre as 64 artes que toda mulher devia conhecer[4]. Por volta de 800 d.C. haviam inúmeras cifras de substituição simples sendo usadas para os mais variados fins, desde o comércio à arte da guerra. Nesta época o estudioso al Kindi[5] desenvolveu uma poderosa técnica criptanalítica: a *Análise de Frequências de Ocorrência de Letras* (ou caracteres).

Para quaisquer dois textos naturais[6], escritos em uma mesma língua, a frequência em que uma dada letra é usada gera porcentagens que se aproximam quanto mais longos são os textos. Em uma análise de muitos textos longos, as letras do alfabeto adquirem uma distribuição de porcentagens bem definida para cada língua, isto permite a compilação de tabelas, uma para cada língua (Figura 1.1).

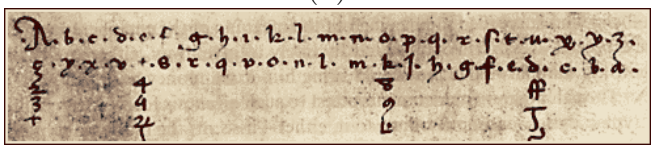
[3] A Cifra de César era a simples troca de cada letra da mensagem por uma letra três posições à frente no alfabeto. Por exemplo, a palavra *zebra* tornava-se *cheud*. Embora a cifra pareça muito fácil de ser quebrada, há que se considerar que muito poucas pessoas sabiam ler naquela época.

[4] 44ª arte - Escrever em cifras: Criptografia; 45ª arte - Falar mudando as formas das palavras: Criptolalia.

[5] *Abu Yusuf Ya'qub ibn Is-haq ibn as-Sabbah ibn 'omran ibn Ismail al-Kindi* (801-873) é conhecido como o *filósofo dos árabes* e o *bisavô da estatística*. Durante sua vida escreveu mais de 290 livros de medicina, astronomia, matemática, linguística e música.

[6] Isto é, não planejados quanto ao uso seletivo de sinônimos que não contenham uma determinada letra, técnica conhecida como *lipografia*.

(a)



(b)

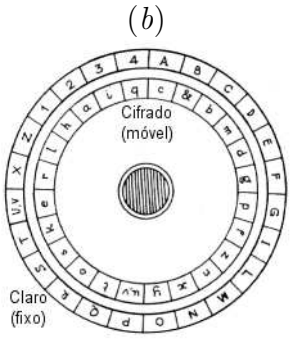


Figura 1.2: (a) Tabela de homófonos de Simeone de Crema, 1401 . (b) O Disco de Alberti, 1466. (Imagens retiradas de [1]).

Nas cifras de substituição simples, cada letra é substituída por um símbolo único. Esta correspondência unívoca garante que cada símbolo mantenha todas as propriedades da letra que substituiu, como a formação de dígrafos com outros símbolos (*ch, lh, qu, rr, ss, etc*) e a frequência de ocorrência no texto. Desta forma, para que seja possível a criptanálise por análise de frequências, basta que seja conhecida a língua em que o texto claro foi escrito e tenha-se em mãos uma tabela com as frequências das letras. Os símbolos no *criptograma* são então contados e, por comparação das porcentagens, grande parte das letras é descoberta.

1.3 1000 anos de avanços

No início do século XIV, o ocidente já conhecia a criptografia e a análise de frequências foi finalmente superada. Os *homófonos*, ou múltiplos substitutos, eram conjuntos de símbolos que, aleatoriamente, tomariam o lugar de uma mesma letra muito frequente, distribuindo sua porcentagem de ocorrência (veja a Figura 1.2.a).

Em 1466, surge o *Disco de Alberti*[7], aceito como a primeira invenção da cifra de substituição polialfabética. O Disco de Alberti é composto por dois discos concêntricos e de tamanhos diferentes. O disco maior é fixo e possui em sua periferia todas as letras em ordem alfabética. O disco menor é livre para girar e possui as letras de forma desordenada. Cada posição do disco menor gera uma nova correspondência letra-letra (ou um novo *alfabeto cifrante* - veja a Figura 1.2.b). O mensageiro escolhe uma letra chave que servirá de referência para a cifragem de todas as palavras. A seguir dispõe o disco interno em uma posição aleatória. Olhando no disco externo, o mensageiro localiza a letra chave e inicia o criptograma escrevendo a

[7] *Leon Battista Alberti (1404-1472)* foi o responsável pelo trabalho considerado mais relevante em um período de 1000 anos na criptografia clássica. Seu tratado, *Tratatti in Cifra*, serviu como base para o trabalho de muitos pesquisadores, dentre eles *Johannes Trithemius (1462-1516)*, *Giambattista Della Porta (1535-1615)* e *Blaise de Vigenère (1523-1596)*. O *Disco de Alberti* foi reinventado em 1867 por *Charles Wheatstone (1802-1875)*, que o considerou uma "invenção genial".

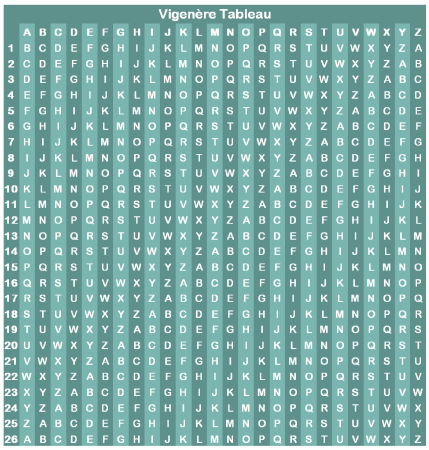


Figura 1.3: O *Quadrado de Vigenère*.

letra correspondente, lida no disco interno. Esta nova letra será a chave da primeira palavra. Com os discos fixos, o mensageiro localiza e transcreve todas as letras da primeira palavra. Para a segunda palavra, o mensageiro dispõe novamente o disco interno em uma configuração aleatória, anota a letra chave da segunda palavra, transcreve a segunda palavra e repete o processo até o fim do texto claro.

O destinatário, conhecendo a letra chave, decifra cada palavra do criptograma através de sua primeira letra, posicionando o disco interno de forma que esta letra se localize abaixo da letra chave.

Como cada palavra é cifrada com um novo alfabeto, a frequência de ocorrência das letras torna-se muito homogênea e impossibilita o uso da análise de frequências para criptanálise. A segurança desta cifra está baseada principalmente no fato de que apenas remetente e destinatário conhecem o mecanismo, ou seja, a configuração das letras no disco cifrante interno. Qualquer terceira pessoa que conheça o mecanismo seria capaz, através de uma busca por tentativa e erro, de descobrir a letra chave e, por conseguinte, ler a mensagem.

1.4 A cifra indecifrável

Em 1586, *Vigenère*[8] publica uma simplificação de sua *cifra de autochave*. A *Cifra de Vigenère* ou também *"Le chiffre indéchiffable"* (a cifra indecifrável), como ficou conhecida, faz uso do *Quadrado de Vigenère*, uma tabela na qual o alfabeto é repetido, mas deslocado de uma casa, a cada linha (veja a Figura 1.3).

[8]Blaise de Vigenère (1523-1596) fez um estudo exaustivo dos trabalhos disponíveis à época e os compilou em seu *Traicté des chiffres*, dando os créditos aos devidos autores. Muitos dos trabalhos originais dos autores desta época foram perdidos e é graças a Vigenère que sabemos de sua existência e autores.

Para usar a Cifra de Vigenère, o mensageiro define uma palavra chave e a compartilha com o destinatário secreta e previamente. A seguir, o texto claro é escrito sem espaços sobre um papel. Acima do texto claro, o mensageiro escreve a palavra chave repetidamente até que todas as letras do texto claro contenham uma letra da chave logo acima. Cada letra da chave define, na primeira coluna, qual linha do Quadrado de Vigenère será usada como alfabeto cifrante. O mensageiro então localiza a letra do texto claro na primeira linha (não numerada) e percorre sua coluna até o alfabeto cifrante. Nesta cifra o número de alfabetos cifrantes usados é o número de letras distintas presentes na palavra chave escolhida.

A supremacia da Cifra de Vigenère teve fim em 1854 quando *Charles Babbage*[9] desenvolveu uma técnica criptanalítica capaz de extrair a chave do criptograma e decifrá-lo.

Babbage notou que o uso repetido da chave poderia levar a repetições no criptograma, caso um mesmo dígrafo do texto claro fosse encriptado pelo mesmo trecho da chave em posições diversas no texto. Uma análise cuidadosa do criptograma revela a repetição de um dado par de letras, e o espaçamento em que aparecem é um múltiplo de um mesmo número - o número de letras da chave. Após o cálculo do mínimo múltiplo comum dos espaçamentos é obtido o comprimento da chave. Os caracteres do criptograma são então separados em grupos, no qual cada grupo contém apenas os caracteres que foram encriptados pela mesma letra da chave (devido à repetição de seu uso). Para cada grupo é aplicada a análise de frequências e se obtém uma distribuição de porcentagens para o alfabeto usado. Os alfabetos da Cifra de Vigenère são apenas deslocamentos do alfabeto original, assim, o gráfico da distribuição obtido para cada grupo pode ser arrastado até que se ajuste na distribuição original da língua. O número de casas deslocadas para cada grupo é a posição da respectiva letra da palavra chave no alfabeto.

1.5 A invenção do rádio: sistemas abertos de comunicação

A partir de 1894, Guglielmo Marconi (1874-1937) estudou os princípios elementares de uma transmissão telegráfica e teve sucesso na transmissão de código Morse através do Canal da Mancha em 1899, dando assim início à era da comunicação sem fios[10]. O uso de ondas de rádio

[9]Charles Babbage (1791-1871) é considerado "o pai do computador" por seus projetos da *Máquina das Diferenças n^o 1*, *n^o 2* e da *Máquina Analítica*. Apesar do amplo financiamento recebido, Babbage nunca concluiu a construção destas máquinas. Apenas em 1991 o London Science Museum utilizou os projetos originais de Babbage e construiu a *Máquina das Diferenças n^o 2* simulando a precisão de usinagem disponível no século 19. A máquina funcionou perfeitamente, sendo capaz de armazenar 7 números com 31 dígitos cada e, portanto, calcular polinômios de sétimo grau com 31 dígitos de precisão.

[10]O padre brasileiro Roberto Landell de Moura (1861-1928) realizou experimentos a partir de 1892 e realizou transmissões públicas de voz humana em 1899, noticiadas pelo jornal O Estado de S. Paulo. Suas

implica no uso de canais de comunicação verdadeiramente abertos pois qualquer indivíduo suficientemente próximo à antena emissora tem a possibilidade de captar seus sinais. A transmissão a longas distâncias de informações confidenciais passaria então a *exigir* o uso de criptografia.

A captação e decifração do telegrama de Zimmermann, em 16 de janeiro de 1917, é exemplo de como a criptografia é capaz de alterar a história humana, sendo o pretexto dos EUA para seu ingresso na 1ª Guerra Mundial. Arthur Zimmermann, ministro das relações exteriores do Império Alemão, redigira o telegrama com o objetivo de firmar uma aliança com o México, garantindo-lhe armamentos e a reconquista dos territórios do Texas, Arizona e Novo México em troca de ataques aos EUA, caso eles entrassem na guerra. Dentro de um mês a publicação do telegrama de Zimmermann mudou a opinião pública norte-americana, que antes era neutra em relação à guerra, resultando no ingresso dos EUA na guerra.

1.6 O *one-time-pad*

Ainda em 1917, *Gilbert Sandford Vernam* (1890-1960), da AT&T Bell Labs, propôs uma cifra em que o texto claro era combinado caractere por caractere com uma chave tão comprida quanto o texto. Pouco tempo depois, o então capitão *Joseph Oswald Mauborgne* (1881–1971) propôs que a chave, ao invés de ser composta por outro texto ou frases, poderia ser uma sequência aleatória de caracteres, dificultando mais a criptanálise. A união destas idéias tornou-se conhecida como *One-Time-Pad*, pois a chave, escrita sobre uma fita de papel facilmente destrutível, nunca deveria ser reutilizada para a encriptação de mensagens. No one-time-pad a combinação é feita através de um processo similar à Cifra de Vigenère, com o uso de *aritmética modular*[11]. A cada letra do alfabeto associamos um número de 0 a 25. A combinação do texto claro com a chave é feita pela adição destes números módulo 26. A reobtenção do texto claro, a partir do criptograma, é feita através da subtração da chave módulo 26 (veja as Figuras 1.4.*a* e *b*).

Em 1949, quase trinta anos mais tarde, *Claude Elwood Shannon* (1916-2001)[12], também

descobertas foram completamente ignoradas pelas autoridades brasileiras da época e hoje a polêmica da invenção do rádio se compara à da invenção do avião. Apenas em 1914 Marconi transmitiu voz humana em seus equipamentos. Nikola Tesla (1856-1943) também lutou, sem sucesso, pela "paternidade" do radio.

[11] A aritmética modular, aritmética do relógio ou calculadora-relógio, utiliza apenas o resto da divisão por um dado número para o cômputo das operações básicas. Escrevemos a afirmação "o resto da divisão de 7 por 4 é três" na forma $7(\mathbf{mod}\,4) = 3$. Outros exemplos são: $5(\mathbf{mod}\,11) = 5$; $15(\mathbf{mod}\,3) = 0$; $12(\mathbf{mod}\,5) = 2$; $(7 \times 5)(\mathbf{mod}\,4) = [7(\mathbf{mod}\,4)] \times [5(\mathbf{mod}\,4)]\mathbf{mod}\,4 = 3$; etc [43].

[12] Shannon é considerado o fundador da *Teoria de Informação* por seu *paper "A Mathematical Theory of Communication"* de 1948. Shannon estabeleceu os elementos básicos de um sistema de comunicação, os conceitos de *entropia informacional* e *redundância* e introduziu o termo *bit* como unidade de medida de informação [43, 8]. A entropia de uma sequência mede as correlações entre diferentes partes dessa sequência.

	A 0	*B* 1	*C* 2	*D* 3	*E* 4	*F* 5	*G* 6	*H* 7	*I* 8	*J* 9	*K* 10	*L* 11	*M* 12	*N* 13	*O* 14	*P* 15	*Q* 16	*R* 17	*S* 18	*T* 19	*U* 20	*V* 21	*W* 22	*X* 23	*Y* 24	*Z* 25	
(*a*)		08	(I)		15	(P)			01	(B)		22	(W)		12	(M)											Chave
		05	(F)		08	(I)			16	(Q)		20	(U)		04	(E)											Mensagem
		13			23				17			42			16												Chave + Mensagem
		13	(N)		23	(X)			17	(R)		16	(Q)		16	(Q)											(Chave + Mensagem) (mod 26)
(*b*)		13	(N)		23	(X)			17	(R)		16	(Q)		16	(Q)											Criptograma
		-08	(I)		-15	(P)			-01	(B)		-22	(W)		-12	(M)											- Chave
		05			08				16			-06			04												Criptograma - Chave
		05	(F)		08	(I)			16	(Q)		20	(U)		04	(E)											(Criptograma - Chave) (mod 26)
(*c*)		13	(N)		23	(X)			17	(R)		16	(Q)		16	(Q)											Criptograma
		-18	(S)		-09	(J)			-06	(G)		-23	(X)		-12	(M)											- "Chave"
		-05			14				11			-07			04												Criptograma - "Chave"
		21	(V)		14	(O)			11	(L)		19	(T)		04	(E)											(Criptograma - "Chave") (mod 26)
(*d*)		13	(N)		23	(X)			17	(R)		16	(Q)		16	(Q)											Criptograma
		-18	(S)		-19	(T)			-04	(E)		-09	(J)		-16	(Q)											- "Chave"
		-05			04				13			07			00												Criptograma - "Chave"
		21	(V)		04	(E)			13	(N)		07	(H)		00	(A)											(Criptograma - "Chave") (mod 26)

Figura 1.4: Cifragem através do One-Time-Pad: (*a*) A mensagem "FIQUE" é cifrada através da sequência aleatória "IPBWM". (*b*) O destinatário utiliza a chave correta e decifra a mensagem. (*c*) e (*d*) Um espião com *poder computacional ilimitado* encontra facilmente diversas chaves que resultam em mensagens igualmente válidas (incluindo a mensagem correta), mas não possui informações suficientes para decidir qual é a verdadeira [43].

da Bell Labs, provou matematicamente que o one-time-pad é *incondicionalmente seguro*, pois o criptograma isolado não possui nenhuma informação sobre o texto claro (veja as Figuras 1.4.*b*, *c* e *d*). Shannon demonstrou ainda que toda e qualquer cifra que pretenda manter-se permanentemente indecifrável *deve* assemelhar-se ao one-time-pad.

A chave utilizada no one-time-pad deve ser constituída por uma sequência *verdadeiramente aleatória* de caracteres. Um algoritmo implementado por um código de comprimento finito nunca será capaz de gerar mais *entropia* do que aquela contida em seu código, ou seja, a chave gerada por ele não será completamente aleatória e conterá inúmeros vínculos exploráveis por um poder computacional ilimitado[13]. Tais algoritmos são chamados *geradores de números pseudo-aleatórios*. A segurança do one-time-pad exige o uso de números *genuinamente aleatórios* e, atualmente, tais números podem ser gerados em computadores através de um *hardware* que faz uso de fenômenos quânticos, como o ruído térmico ou o efeito fotoelétrico [1, 32].

1.7 O problema da distribuição de chaves

Embora incondicionalmente seguro, o one-time-pad *requer* a transmissão secreta de uma chave tão comprida quanto o texto a ser enviado. Esta necessidade leva ao *problema da distribuição de chaves* [32]. A solução mais direta para este problema é o encontro pessoal entre remetente e destinatário. O remetente, portador de duas cópias idênticas de uma dada sequência aleatória de caracteres (ou bits), entrega uma das cópias ao destinatário. Quando, em algum momento posterior, o remetente achar necessário o uso de uma comunicação secreta, ele utiliza o one-time-pad e especifica ao destinatário qual foi o trecho usado da sequência partilhada por eles. Ambos, remetente e destinatário, riscam (ou apagam) o trecho da chave que foi usado, para que ele nunca seja reutilizado.

Esta solução é pouco viável e é impraticável entre indivíduos que não terão a oportunidade de se encontrar antes da necessidade da comunicação secreta. É neste ponto que a *Distribuição Quântica de Chaves* surge como solução, pois permite a transmissão de chaves arbitrariamente grandes entre indivíduos que nunca tenham se encontrado[14].

[13] A medida do comprimento deste menor programa é chamada *Complexidade de Kolmogorov* [17].

[14] Um dos ataques mais comuns da criptografia clássica é o chamado *man-in-the-middle attack* (veja a Seção 8.4.1). Neste ataque o espião comunica-se com o remetente fingindo ser o destinatário e comunica-se com o destinatário fingindo ser o remetente. A mecânica quântica não provê meios para a autenticação entre as partes comunicantes, isso implica a necessidade de que estes indivíduos compartilhem, na verdade, uma pequena quantidade de informação, usada para autenticação (veja a Seção 2.4.4).

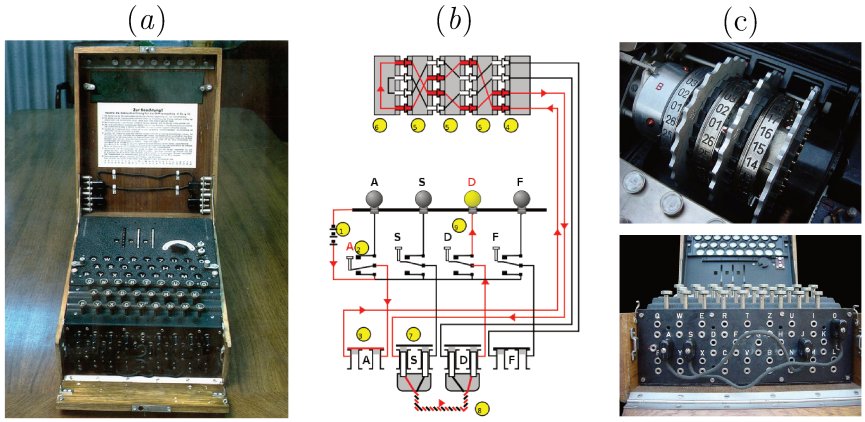


Figura 1.5: (a) Maquina Enigma com três rotores. (b) Ligação elétrica da máquina. (c) Refletor, rotores e plugboard. Cada tecla pressionada gira o rotor mais à direita que, ao completar uma volta, gira o próximo rotor e assim por diante, de forma semelhante a um conta-quilômetros. O plugboard realiza a troca de uma letra por outra em até 13 pares de letras e dificulta imensamente a criptanálise. (Imagens retiradas de [43, 2]).

1.8 As *máquinas Enigma*

Em 1918, *Arthur Scherbius* (1878-1929) patenteou o primeiro modelo da máquina Enigma e tentou, sem sucesso, vendê-la ao exército alemão. A seguir, ele e seu amigo E. Richard Ritter transferiram a patente à *Gewerkschaft Securitas*, que fundou a *Chiffriermaschinen Aktien-Gesellschaft*, empresa fabricante de máquinas cifrantes. Diversas variantes da máquina Enigma surgiram, com codificações cada vez mais complexas, e foram utilizadas por diversos serviços militares e governamentais de vários países. A Alemanha Nazista, em especial, fez amplo uso da Enigma, empregando-a na marinha, exército, forças aéreas e Gestapo. Ainda na Alemanha, a Enigma foi usada por grupos nazistas e por diplomatas [43].

A variação mais comum da Enigma era um dispositivo eletro-mecânico composto por um teclado, um painel de letras que acendiam, um *plugboard*, um refletor e um mecanismo de passo que abrigava de 3 a 8 rotores (veja a Figura 1.5).

Os rotores da Enigma possuiam contatos em ambas as faces e uma interligação diferente entre eles para cada rotor. Cada tecla pressionada movimentava os rotores levando a caminhos elétricos diferentes, o que fazia com que uma mesma letra fosse codificada com um novo alfabeto cifrante a cada pressionamento.

Seu uso era simples e rápido. Um *livro de códigos* definia a chave e a configuração de plugboard a ser usada a cada dia. Após configurada, escolhia-se uma nova chave a cada mensagem e esta chave era digitada duas vezes, para se evitar erros[15]. Novamente reconfigurava-se os

[15]Esta repetição de uma mesma sequência de caracteres foi bastante explorada para a criptanálise da Enigma, pois os pares de caracteres continham vínculos que revelavam a configuração usada na máquina. A

rotores, desta vez na posição da chave escolhida para a mensagem e digitava-se a mensagem. Os livros de códigos da marinha eram impressos em tinta vermelha, solúvel em água, sobre papel rosa, visando sua fácil destruição em caso de captura pelas forças inimigas [43].

1.9 A criptanálise do sistema Enigma

A Enigma se constituia basicamente de uma cifra de substituição polialfabética. O número de configurações possíveis (número de chaves) que a máquina de três rotores podia assumir era de aproximadamente $3 \times 10^{114} \sim 380$ bits, sendo que o roubo de uma dessas máquinas (conhecimento das ligações internas dos 5 discos, dos quais 3 são usados por vez) e o conhecimento da ligação (*jumpeamento*) do plugboard reduzia estas configurações para "apenas" $10^{23} \sim 76$ bits [42].

As primeiras máquinas para a quebra do sistema Enigma foram as *Bombe Machines*, projetadas pelas grandes mentes de Alan Turing e Gordon Welchman, entre outros, e sendo uma grande fonte de informações para a ULTRA (a inteligência inglesa e norte-americana [43]). As Bombe machines simulavam os rotores da Enigma, fazendo testes automatizados de chaves [43].

Com o desenrolar da guerra, novos sistemas criptográficos foram desenvolvidos, dentre eles as *Lorenz Machines*, de complexidade muito incrementada. As últimas máquinas construídas para a busca de suas chaves foram as *Colossus Machines* (1944), os primeiros computadores eletrônicos digitais do mundo, programáveis através de um plugboard e cabos de jumpeamento. A primeira Colossus machine foi projetada e parcialmente construída pelo engenheiro britânico Tommy Flowers, sendo as máquinas seguintes desenvolvidas pelos engenheiros Allen Coombs, Harry Fensom, Sid Broadhurst e Bill Chandler [43].

1.10 O Mundo Digital

A criptanálise dos criptogramas transmitidos durante a Segunda Guerra Mundial representa o primeiro uso massivo de poder computacional da história. A partir destes esforços, novas arquiteturas de computadores foram criadas para propósitos mais gerais, como o ENIAC (1946) e o Manchester Mark 1 (1949) [43]. Em paralelo, o desenvolvimento de novas tecnologias, como o transistor (1947/1948), possibilitou a miniaturização e a grande disseminação dos computadores que, por fim, se tornariam os terminais de acesso a um mundo virtual de informações: a internet. É neste admirável mundo novo que recuperamos aquela antiga necessidade humana: a criptografia.

---

partir de 1940 o uso da Enigma foi modificado.

Capítulo 2

Os Elementos da Criptografia Moderna

Neste capítulo serão apresentados os fundamentos da criptografia moderna convencional. Será apresentada uma modelagem do Sistema de Comunicação, a importância e tipos de cifras com chave, e o procedimento de autenticação do remetente, tão essencial à Distribuição Quântica de Chaves. Mais adiante, no Capítulo 7, veremos técnicas de correção de erros na chave e técnicas de redução do conhecimento que um possível espião possa ter da chave (ampliação de privacidade).

2.1 O sistema de comunicação

Em 1949, Shannon notou que um sistema de comunicação secreta poderia ser modelado por seis elementos básicos: a fonte de informações, a fonte de chaves, o cifrador, os canais de transmissão, o decifrador e o receptor das mensagens (veja a Figura 2.1). A imperfeição do canal (ou espionagem) pode causar alterações no sinal transmitido, modeladas por uma fonte de ruídos.

Um estudo mais detalhado do canal de transmissão, de sua capacidade e da informação transmitida será realizado no Capítulo 3. A seguir apresentamos os outros elementos deste sistema.

2.2 *Dramatis personae*

O drama da criptografia através do sistema de comunicação envolve três famosos personagens [16]:

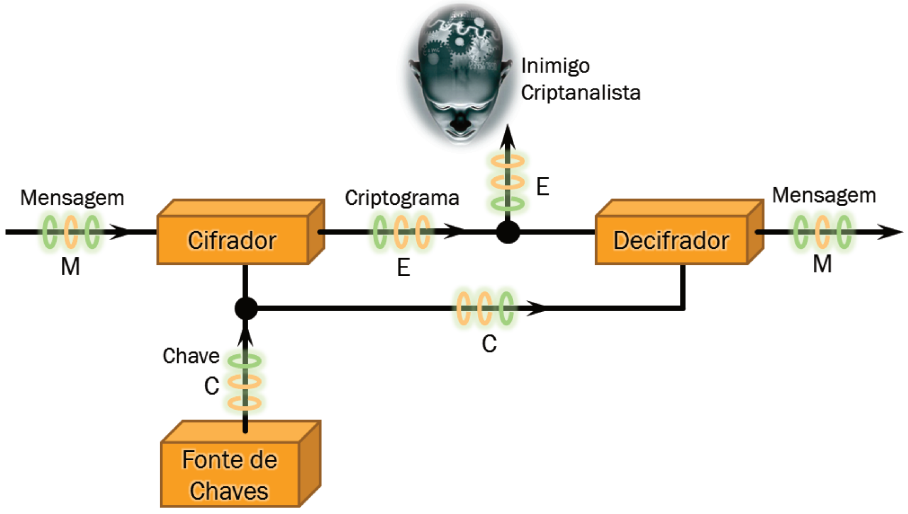


Figura 2.1: Modelagem de um sistema de comunicação secreta. A fonte de informações gera a mensagem, que é combinada com a chave através de uma cifra. O canal público carrega o criptograma e é espionado. A chave deve ser entregue por um meio seguro. O destinatário usa a chave e decifra a mensagem, que então pode ser lida [9].

Alice, a emissora das mensagens cifradas;

Bob, o destinatário; e

Eva, a espiã.

Alice e Bob são a fonte e o destinatário e têm sob seu comando o transmissor e o receptor de sinais, respectivamente. Assume-se que toda a extensão do canal fica exposta a qualquer tentativa de espionagem por parte de Eva, que pode então fazer uso de quaisquer técnicas de medição, sondagem, transmissão, inferência, etc., permitidas pelas leis da física quântica, introduzindo (ou mesmo reduzindo) ruídos no sinal transmitido.

2.3 O princípio de Kerckhoffs

O desenvolvimento das técnicas criptográficas modernas levou à concepção de princípios-guia para o desenvolvimento de cifras mais práticas, seguras e de fácil distribuição. Um destes princípios é o Princípio de Kerckhoffs:

"A segurança de um sistema criptográfico não deve depender do fato de o algoritmo ser secreto ou não. Ela deve ser garantida apenas por se manter secreta a chave."

O código-fonte das cifras modernas são distribuídos livremente pela internet, de forma que qualquer indivíduo possa fazer uso destas técnicas criptográficas (ou mesmo melhorá-las).

Por este motivo, um possível espião tem também acesso à estrutura da cifra. Entretanto, graças à maneira como a cifra foi desenvolvida, de acordo com o princípio de Kerckhoffs, a mensagem cifrada permanece segura [2, 43].

2.3.1 A máxima de Shannon

O princípio de Kerckhoffs foi resumido e simplificado por Shannon em uma afirmação única:

"O inimigo conhece o sistema."

2.3.2 O Cenário Paranóico

Em um cenário realista o canal é imperfeito e introduz distorções e perdas no sinal transmitido. Uma ação de espionagem simples, como a divisão do sinal em duas partes[1], uma a ser medida pelo espião e a outra a ser transmitida a Bob, causa perdas no sinal. Esta perda é confundida com a perda natural da transmissão, o que mascara a espionagem. Além disso, um espião com grandes recursos tecnológicos poderia remover apenas a parte do sinal que seria perdida durante uma transmissão normal e transmitir, sem perdas (graças aos avançados recursos tecnológicos que ele possuiria), o restante do sinal a Bob. Para Bob e Alice este tipo de espionagem seria indetectável. Para que uma cifra possa ser incondicionalmente segura, ela deve resistir a qualquer ataque existente ou possível de ser realizado no futuro. Desta forma, o título "incondicionalmente segura" só é dado às cifras que permanecem seguras mesmo quando supomos que Eva tem acesso a todo o canal quântico, possui *tecnologia ilimitada*[2] e tem acesso a todas as transmissões pelo canal clássico (públicas). Tais considerações compõem o chamado *Paranoidal Picture*.

2.4 Criptografia Computacional

Com o desenvolvimento dos computadores, a transmissão de informações passou a ser feita de forma digital e as cifras passaram a ser desenvolvidas na forma de softwares, implementando algoritmos especialmente projetados para computadores. Nesta seção apresentaremos os conceitos mais importantes nos quais se baseiam estas cifras modernas [2, 1, 19].

[1] por exemplo através de um divisor de feixes, como será estudado adiante, no caso de sinais luminosos.

[2] Ilimitada dentro das possibilidades definidas pelas leis da natureza (mecânica quântica). Uma tecnologia ilimitada inclui poder computacional ilimitado, permitindo ao espião quebrar todas as cifras baseadas na segurança computacional prática (DES, AES, RSA, etc).

2.4.1 Criptografia de Chaves Simétricas

Nas cifras de chaves simétricas o emissor e o receptor possuem a mesma chave. Esta chave define os parâmetros que regem o embaralhamento da mensagem, realizado pelo algoritmo escolhido.

Os processos de encriptação e decifração das mensagens são implementados com alto desempenho nestas cifras, chegando a taxas de Gb/s, mas há uma necessidade constante de renovação das chaves. Estas chaves devem ser geradas e distribuídas em segurança e a criptografia de chaves simétricas não permite a autenticação do remetente.

Exemplos dessas cifras são o DES (Data Encryption Standard 1976-1999, hoje inseguro), o Triple-DES, o IDEA, o RC (*Rivest Cipher* - muito usado em e-mails), o Twofish, o Blowfish e o AES (Advanced Encryption Standard) [43].

2.4.2 Criptografia de Chaves Assimétricas (ou Chaves Públicas)

Nestas cifras são usadas duas chaves distintas, uma pública e uma privada, ambas geradas pelo destinatário da mensagem. Uma das chaves é publicada pelo destinatário para todos que queiram se comunicar com ele e funciona como um cadeado. Seu uso no algoritmo cifrante altera a mensagem em uma direção única, de forma que nem mesmo o próprio emissor consegue decifrá-la. A chave privada, guardada pelo destinatário, atua revertendo estas alterações.

Cada algoritmo que realiza a transformação do texto claro em criptograma, e não permite um retorno simples, é composto por uma função matemática chamada de *função de via única*. Tais funções são simples de serem calculadas em um sentido, mas sua inversa é bem mais exigente em termos computacionais. Como exemplo, quase qualquer pessoa é capaz de realizar o produto entre números primos 173×281 em poucos segundos, mas descobrir quais são os dois fatores primos do número 50629 é uma tarefa um pouco desgastante. Esta tarefa de fatoração não é difícil apenas para humanos, é também uma tarefa formidável para os mais avançados sistemas computacionais atuais (com a diferença de que para estes, os números a serem fatorados possuem 200 dígitos ou mais) [1, 43].

As duas mais famosas cifras de chaves assimétricas são baseadas nesta dificuldade de fatoração: o RSA e o El Gamal[3]. A busca destes fatores primos seria bastante simplificada com o desenvolvimento de um algoritmo capaz de gerar números primos enormes e rotulados conforme sua posição na lista de todos os números primos, permitindo assim uma busca

[3]Na realidade o El Gamal está baseado nas dificuldades que o problema do logaritmo discreto pode apresentar. Entretanto, recentemente foi descoberto que uma quebra da cifra RSA também permite quebrar o El Gamal, devido ao uso de números primos e aritmética modular e sua relação com o problema do logaritmo discreto.

mais direta. Atualmente não se tem notícia do desenvolvimento bem sucedido de tal algoritmo, razão pela qual acredita-se que estas cifras permanecem seguras do ponto de vista computacional.

A grande utilidade das cifras de chaves assimétricas é a possibilidade de troca de chaves seguras entre partes que nunca puderam se comunicar previamente, mas essa segurança é uma *segurança computacional prática* e não incondicional.

2.4.3 Criptografia Hash

Uma função Hash (do inglês "picar, misturar") atua transformando uma grande quantidade de informação em uma pequena quantidade de informação através de uma mistura e combinação dos bits de forma bastante complexa. Devido à redução no comprimento da sequência de bits de entrada, várias entradas deverão corresponder a uma mesma saída, o que é chamado de *colisão*. Isto impossibilita a reobtenção da sequência de entrada quando apenas se conhece a saída. Quanto mais difícil é a geração de colisões intencionais, melhor é o algoritmo [43].

As saídas das funções Hash possuem um comprimento fixo de 128, 160 ou mais bits, e são usadas como rotulação para identificar os arquivos transmitidos pela internet. Por exemplo, a verificação da integridade de um documento PDF baixado em seu computador pode ser feita através da comparação do valor Hash calculado para o arquivo em seu computador e no servidor de internet. Outros dois exemplos de procedimentos que fazem uso das funções Hash são a autenticação do remetente, descrito na seção seguinte, e a ampliação de privacidade, descrita na Seção 7.5.

Existem vários tipos de função Hash disponíveis atualmente, dentre elas temos o SHA (Secure Hash Algorithm), e o MD (Message Digest Algorithm).

2.4.4 A Autenticação do Remetente

Devido à facilidade de cópia, interceptação e alteração das mensagens transmitidas, especialmente pela internet, logo foi necessário o desenvolvimento de sistemas de assinatura digital capazes de comprovar se as mensagens recebidas realmente foram enviadas por determinado remetente.

Para efetuar a assinatura digital de uma mensagem, o emissor calcula um resumo da mensagem (Hash) e encripta este valor com uma chave privada, gerada por ele mesmo juntamente com uma chave pública. Neste caso é a chave privada que serve como cadeado. O valor hash encriptado é a assinatura da mensagem e será transmitido juntamente com ela ao destinatário. Este, por fim, calcula o hash da mensagem e também decifra o hash recebido. Se os dois valores hash forem diferentes, ou a mensagem foi alterada após a sua assinatura

ou a chave usada para sua encriptação não foi a chave privada do verdadeiro emissor [43].

A autenticação do remetente permite uma solução aos ataques do tipo Man-in-the-Middle (Seção 8.4.1).

2.5 Computação Quântica: O fim da segurança computacional prática

Em 1994, Peter Shor descobriu um algoritmo, a ser rodado em um computador quântico, capaz de fatorizar números inteiros em seus fatores primos em um tempo exponencialmente menor que os melhores algoritmos clássicos conhecidos. Esta grande capacidade de paralelização dos computadores quânticos irá pôr à prova os mais utilizados sistemas criptográficos da atualidade, invalidando a tão confiada segurança computacional prática [18, 2, 43]. Este problema para a criptografia moderna é apenas um avanço natural da própria criptografia, já que os primeiros protocolos incondicionalmente seguros, baseados na mecânica quântica, surgiram mesmo antes das primeiras ocorrências de quebras das cifras computacionais clássicas.

Nos capítulos seguintes desenvolveremos o ferramental teórico necessário à compreensão dos protocolos de Distribuição Quântica de Chaves (QKD) com variáveis contínuas, a serem apresentados, juntamente com dois protocolos de variáveis discretas, na terceira parte deste texto.

Parte II

A Matemática, Física e Tecnologia da Criptografia Quântica

Capítulo 3

A Informação E Sua Quantificação

Neste capítulo serão introduzidos os conceitos de informação e entropia no âmbito da teoria de informação, além do cálculo da informação mútua. A aquisição desses conceitos é fundamental para uma boa compreensão das técnicas de correção de erros e ampliação de privacidade, e o cálculo da informação mútua será útil na análise de segurança dos protocolos apresentados mais adiante.

Para definirmos e quantificarmos a informação, podemos tentar partir de nossa intuição ou do senso comum. Parece razoável a noção de que informação é aquilo que está contido em um texto descritivo. Este texto, composto em uma linguagem tão complexa quanto se queira, baseia-se nas experiências da consciência que o escreve, e esta consciência, com os sentidos tão aguçados quanto seja possível, só pode notar o que é distinguível. Concluímos, de certa forma, que informação é distinguibilidade.

Observando que o número mínimo de objetos que permite distinção é dois, em 1948 Shannon percebeu que toda e qualquer informação poderia ser armazenada ou transmitida através de uma linguagem muito simples: a *linguagem binária* [8].

3.1 A linguagem binária

Devido à distinguibilidade, é possível a formulação de perguntas com respostas do tipo "sim" (1) ou "não" (0) (binárias). Isto permite a transmissão de qualquer informação. Como exemplo, considere que seu amigo gostaria de saber a cor do sofá de sua casa. Uma sequência de perguntas do tipo {"É verde?", "É azul?", "É vermelho?"} poderia levar à sequência de resposta {001}, indicando que o sofá é vermelho. Da mesma forma, a localização de um objeto pequeno em uma grande sala pode ser feita através de apenas 10bits a 15bits, com 10 a 15 perguntas do tipo "Dividindo a sala ao meio, o objeto estaria à esquerda?", "Dividindo ao meio, estaria na parte de cima?", etc. Estas perguntas podem ser combinadas de antemão

e, uma vez combinadas, a localização de qualquer novo objeto ou informação de cor pode ser transmitida pelo uso de poucos bits. A representação, transmissão, processamento e armazenagem de dados pelos computadores é feita de forma análoga.

3.2 Entropia de Shannon de uma variável aleatória

A entropia[1] é uma medida da incerteza que possuímos sobre o conhecimento de uma dada variável aleatória [17]. Chamemos de X uma variável aleatória discreta com alfabeto $\mathcal{X}$ e função de probabilidade $p_X(x) = Pr\{X = x\}, x \in \mathcal{X}$.[2] Para simplificar chamaremos $p_X(x) = p(x)$, ficando implícito que $p(y) = p_Y(y)$. A entropia $H(X)$ de uma dada variável aleatória discreta X é dada por:

$$H(X) = -\sum_{x \in \mathcal{X}} p(x) \log_2 p(x) \tag{3.2.1}$$

Usa-se a convenção de que $0 \log_2 0 = 0$, em concordância com a continuidade desta função e com o fato de que a adição de termos com zero probabilidade não altera a entropia. Quando utiliza-se o logaritmo na base 2, a entropia é dada em *bits* (*binary digits*), e quando se utiliza a base natural e, a unidade é o *nat* (*natural digit*). Neste texto, calcularemos as entropias em bits.

Para um *ensemble* de escolhas da variável aleatória X, o cálculo da entropia permite a obtenção de uma média dos menores números de bits necessários para a representação (transmissão, etc) do resultado destas escolhas. A minimização da sequência de bits transmitida está associada à escolha dos significados que os valores destes bits terão para emissor e receptor. A escolha deste sistema de representação da informação é uma busca cega que pode ser guiada pelo valor calculado para a entropia de Shannon. Quanto mais próximo da entropia estiver a média, sobre o *ensemble*, do número de bits usados na comunicação, melhor é o conjunto de perguntas escolhido. O exemplo a seguir irá esclarecer melhor estes conceitos [17].

Exemplo

Transmitindo uma corrida de cavalos

[1] Diz-se que a denominação "entropia" foi uma sugestão de *John Von Neumann (1903-1957)* para Shannon por dois motivos: pela semelhança da expressão com a da entropia e porque, conforme teria dito, "em uma discussão você terá uma vantagem sobre seus adversários, pois ninguém entende direito o conceito de entropia".

[2] x é a representação de um valor da variável aleatória ainda não escolhido. $\mathcal{X}$ é o conjunto de valores (símbolos). Por exemplo, para uma variável binária temos $\mathcal{X} = \{0, 1\}$ e $x = 0$ ou $x = 1$. A representação X já engloba a função de probabilidades $p_X(x)$, que rege o aparecimento dos valores $x \in \mathcal{X}$.

Suponha que um jornalista foi enviado para noticiar uma certa corrida de cavalos, onde 4 cavalos (a, b, c e d) competem pelo prêmio. O histórico passado de vitórias e derrotas destes cavalos foi analisado e foi montada uma tabela com as probabilidades que cada cavalo tem de ser vitorioso:

$$X = \begin{cases} a, \text{ com probabilidade } \frac{1}{2} \\ b, \text{ com probabilidade } \frac{1}{4} \\ c, \text{ com probabilidade } \frac{1}{8} \\ d, \text{ com probabilidade } \frac{1}{8} \end{cases} \tag{3.2.2}$$

Suponhamos agora que o resultado da corrida deva ser informado à central jornalística através do menor número possível de perguntas com as respostas possíveis "sim" ou "não" (perguntas binárias). Uma sequência destas perguntas pode ser combinada previamente com o correspondente ainda no estúdio. Desta forma, terminada a corrida, basta que o correspondente envie ao estúdio uma curta sequência de bits, onde cada bit responde a uma pergunta (0 = não, 1 = sim).

As questões que surgem neste problema são: Quais seriam as melhores perguntas a serem feitas? e Qual é o menor número de bits necessário?

Como tentativa (bem informada) tentaremos a sequência de perguntas: "O cavalo ganhador foi o a?", "O cavalo ganhador foi o b?","O cavalo ganhador foi o c?". Desta forma, a vitória de cada cavalo define uma sequência diferente de bits e temos as seguintes possibilidades e probabilidades de respostas:

Ganhador	Transmissão	No. bits usados	Probabilidade
a	1	1	1/2
b	01	2	1/4
c	001	3	1/8
d	000	3	1/8

Considerando um grande *ensemble* de tais corridas (ou um longo campeonato com os mesmos cavalos), o correspondente enviará ao estúdio o número médio de:

$$N_{bits} = 1 \cdot \frac{1}{2} + 2 \cdot \frac{1}{4} + 3 \cdot \frac{1}{8} + 3 \cdot \frac{1}{8} = \frac{7}{4} \text{ bits} \tag{3.2.3}$$

desta forma, a média de bits necessários para a determinação do ganhador da corrida seria de 7/4 bits para a sequência de perguntas escolhida.

A entropia de Shannon da variável aleatória X nos fornece o menor número médio de bits necessários para sua representação. Para o caso considerado, a entropia é dada por:

$$H(X) = -\frac{1}{2}\log_2\frac{1}{2} - \frac{1}{4}\log_2\frac{1}{4} - \frac{1}{8}\log_2\frac{1}{8} - \frac{1}{8}\log_2\frac{1}{8} = \frac{7}{4}\text{ bits} \tag{3.2.4}$$

E concluímos que a sequência de perguntas escolhida fornece um esquema 100% eficiente para o caso considerado.

Na computação atual, a busca pela "sequência de perguntas" que minimiza a quantidade de bits necessários para a transmissão de uma mesma informação levou ao desenvolvimento de padrões internacionais para a representação binária de textos (*e.g.* codificação de caracteres ASCII), imagens (*e.g.* formato Bitmap) e áudio (*e.g.* formato Wave), entre outros tipos de arquivos [43].

3.3 Compressão de dados e redundância de uma língua

Programas de compactação de dados como o WinZip®, 7-Zip ou WinRar® buscam por repetições de uma mesma sequência de bits (*e.g.* palavras e tags de formatação) nos dados a serem compactados e trocam cada ocorrência por uma pequena sequência de bits para indicação. Ao final do arquivo é anexado um catálogo com uma cópia única de cada trecho repetido. A descompactação é feita pela substituição de cada indicação pelo trecho original guardado no catálogo [28].

Em um teste com dois documentos de texto no formato TXT, um composto pela repetição da palavra "palavra" e outro contendo o primeiro capítulo do livro "O Alienista", de Machado de Assis, a compactação para o formato ZIP reduziu o primeiro documento de 5928 para 33 bytes (0,56% do tamanho) e o segundo de 5928 para 3027 bytes (51,06% do tamanho), demonstrando que no primeiro texto a redundância é muito maior.

Para as línguas naturais, em geral, temos sempre redundância devido à estrutura da língua, que leva ao uso de diversas palavras de ligação, grandes palavras e flexões de uma mesma palavra. Desta forma, através de uma língua (bem) planejada, a mesma quantidade de informação poderia ser transmitida ou armazenada com o uso de um número menor de palavras pequenas. A redundância do inglês, quando se utilizam as probabilidades de formação de estruturas para até oito letras, é de cerca de 50%, significando que metade do que é escrito é determinado pela estrutura da língua e o autor é livre para escolher apenas

metade dos caracteres [8]. Atualmente, para dificultar a criptanálise, as mensagens a serem enviadas são compactadas antes de serem cifradas.

A entropia de Shannon é uma medida da quantidade irredutível de informação contida em uma mensagem, imagem ou qualquer sequência de bits.[3]

3.4 Entropia conjunta e entropia condicional

Podemos fazer a expansão da definição de entropia para um par de variáveis aleatórias. Para isso consideramos o par (X, Y) como sendo uma nova variável aleatória com função de probabilidade $p(x, y)$ e alfabeto $\mathcal{X} \otimes \mathcal{Y}$. Esta é a chamada *entropia conjunta* [17]:

$$H(X, Y) = -\sum_{x \in \mathcal{X}} \sum_{y \in \mathcal{Y}} p(x, y) \log_2 p(x, y) \tag{3.4.1}$$

Podemos também definir a entropia de uma variável condicionada à escolha de outra, ou *entropia condicional*, como sendo o valor esperado entre os valores da entropia das distribuições condicionadas, ou seja, a média ponderada pelas probabilidades de ocorrência da variável condicionante. A entropia média que resta para Y, condicionada ao conhecimento de X é:

$$\begin{aligned} H(Y|X) &= \sum_{x \in \mathcal{X}} p(x) H(Y|X = x) \\ &= -\sum_{x \in \mathcal{X}} p(x) \sum_{y \in \mathcal{Y}} p(y|x) \log_2 p(y|x) \\ &= -\sum_{x \in \mathcal{X}} \sum_{y \in \mathcal{Y}} p(x, y) \log_2 p(y|x) \end{aligned} \tag{3.4.2}$$

Onde usamos o fato de que a probabilidade conjunta de ocorrência de dois eventos relacionados é o produto da probabilidade de ocorrência de um dos eventos pela probabilidade de ocorrência do outro, caso o primeiro ocorra:

$$p(x, y) = p(x) p(y|x) \tag{3.4.3}$$

[3] A *Complexidade de Kolmogorov* é considerada uma entidade mais fundamental que a entropia de Shannon. A complexidade de uma sequência de dados pode ser definida como sendo o comprimento do menor programa binário de computador capaz de calcular a sequência completa. Desta forma, a complexidade do número π é finita, pois qualquer um de seus dígitos pode ser calculado por um programa de comprimento finito. A complexidade de Kolmogorov e a entropia de Shannon são aproximadamente iguais para uma sequência verdadeiramente aleatória [17].

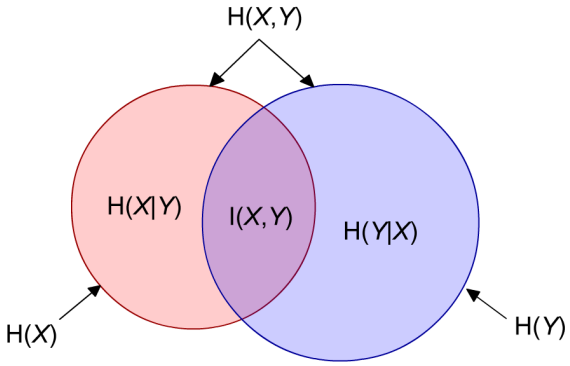


Figura 3.1: Diagrama de Venn das entropias, entropia conjunta, entropias condicionais e informação mútua. Do diagrama obtemos relações do tipo $I(X;Y) = H(X) + H(Y) - H(X,Y)$. Como $I(X;X) = H(X)$, a entropia de uma variável aleatória é também chamada de *self-information* (auto-informação, em tradução livre) [17].

3.5 Definição e quantificação da Informação Mútua

A informação mútua é uma medida da quantidade de informação que uma variável aleatória possui sobre outra variável aleatória. $I(X;Y)$ é a redução da incerteza da variável X graças ao conhecimento da variável Y (e *vice-versa*):

$$
\begin{aligned}
I(X;Y) &= H(X) - H(X|Y) && (3.5.1)\\
&= -\sum_x p(x)\log_2 p(x) + \sum_{x,y} p(x,y)\log_2 p(x|y) && (3.5.2)\\
&= -\sum_x \sum_y p(x,y)\log_2 p(x) + \sum_{x,y} p(x,y)\log_2 \frac{p(x,y)}{p(y)} && (3.5.3)\\
&= \sum_x \sum_y p(x,y)\left[\log_2 \frac{p(x,y)}{p(y)} - \log_2 p(x)\right] && (3.5.4)\\
&= \sum_{x,y} p(x,y)\log_2 \frac{p(x,y)}{p(x)\,p(y)} && (3.5.5)
\end{aligned}
$$

Onde na segunda linha usamos $p(x) = \sum_y p(x,y)$ e a relação [Eq. 3.4.3].

O diagrama de Venn na Figura 3.1 mostra a relação entre as entropias, entropia conjunta, entropias condicionais e informação mútua.

3.6 O Canal de Comunicação e a Capacidade do Canal

O canal de comunicação é um sistema em que a saída depende probabilisticamente da entrada. É caracterizado por uma matriz de probabilidades de transição $p(y|x)$ que determina

a distribuição de probabilidades de saída condicionadas a uma dada entrada. A distribuição de probabilidades de entrada, $p(x)$, é de livre escolha do emissor. A partir dela e das características do canal obtemos as probabilidades conjuntas $p(x,y) = p(x)\,p(y|x)$ e calculamos a informação mútua por sinal transmitido. Ou seja, o acréscimo de informação por sinal transmitido depende da quantidade transmitida de cada símbolo (ou estado). Um código que esteja propenso a fazer maior uso de um dos símbolos permitidos pelo canal será ineficiente, na transmissão de informação pelo canal, com relação a um código que faça um uso bem distribuído dos símbolos (em canal sem perdas).

Definimos a capacidade de um canal como sendo a taxa máxima em que informação pode ser transmitida com probabilidade quase nula de erros. Para um canal com entrada X e saída Y temos:

$$C = \max_{p(x)} I(X,Y) \tag{3.6.1}$$

Onde a maximização é feita pelo ajuste das probabilidades $p(x)$. A esquematização do canal depende do número de símbolos possíveis e das taxas de erros envolvidas [16]. A seguir discutimos quatro exemplos simples.

Exemplo 1

Canal Binário Simétrico (*Binary Symmetric Channel*)

O canal binário simétrico é o exemplo mais básico de um canal com ruído [16, 17]. O sinal transmitido pode estar em apenas um de dois estados (binário). A transmissão pode alterar o sinal de um estado para outro, introduzindo erros (ruído). A modelagem é feita pelo esquema da Figura 3.2, onde estão representadas as probabilidades de sucesso ou não na transmissão. Este tipo de canal é completamente caracterizado pela taxa de erros δ que introduz. As probabilidades devem estar todas normalizadas $\sum_{x,y} p(x,y) = \sum_x p(x) = \sum_y p(y) = 1$.

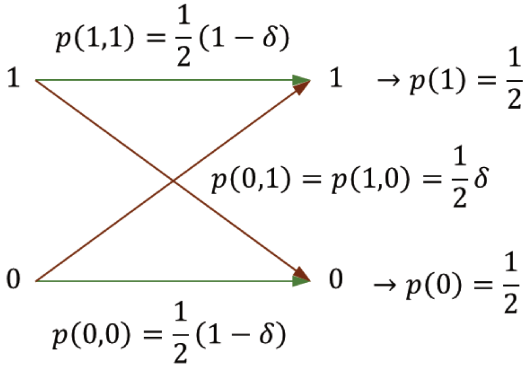


Figura 3.2: Canal Binário Simétrico (*Binary Symmetric Channel*). A entrada de um símbolo pode levar à saída de outro símbolo, conforme a taxa de erros δ do canal.

A informação mútua acrescentada por cada bit emitido e transmitido com taxa de erros δ é dada por:

$$\begin{aligned} I &= \sum_{x,y=0}^{1} p(x,y) \log_2 \frac{p(x,y)}{p(x)\,p(y)} \\ &= 1 + \delta \log_2 \delta + (1-\delta) \log_2 (1-\delta) \end{aligned} \tag{3.6.2}$$

Exemplo 2

Canal binário simétrico sem ruídos

Para um canal sem ruídos ($\delta = 0$), e transmissão do mesmo número de estados de um tipo e de outro, temos $p(1,1) = p(0,0) = 1/2$, $p(1,0) = p(0,1) = 0$ e $p(1) = p(0) = 1/2$. A informação mútua disponibilizada por cada sinal transmitido é:

$$\begin{aligned} I(X,Y) &= 1 + \delta \log_2 \delta + (1-\delta) \log_2 (1-\delta) \\ &= 1 + 0 + 1 \log_2 1 \\ &= 1 \text{ bit} \end{aligned}$$

Ou seja, para cada sinal transmitido, um bit de informação é transmitido (como seria de se esperar para o uso ótimo de um canal binário sem ruído).

Exemplo 3

Canal binário simétrico completamente ruidoso

Neste caso, um estado transmitido pode chegar como qualquer um dos dois estados com igual probabilidade ($\delta = 1/2$), $p(0,0) = p(0,1) = p(1,0) = p(1,1) = 1/4$, e novamente $p(0) = p(1) = 1/2$. O acréscimo de informação mútua para cada estado transmitido é de:

$$\begin{aligned} I(X,Y) &= 1 + \delta \log_2 \delta + (1-\delta) \log_2 (1-\delta) \\ &= 1 + \frac{1}{2} \log_2 \frac{1}{2} + \left(1 - \frac{1}{2}\right) \log_2 \left(1 - \frac{1}{2}\right) \\ &= 1 - \frac{1}{2} - \frac{1}{2} \\ &= 0 \text{ bit} \end{aligned}$$

Em um canal completamente ruidoso a informação transmitida é completamente per-

dida e não existe um uso ótimo do canal. Neste caso a capacidade do canal é $C = 0$.

Exemplo 4

Canal defeituoso de três símbolos

Considere um canal que permite a transmissão de três símbolos (estados) distintos. Durante a transmissão, dois destes símbolos são "confundidos" pelo canal e acabam misturados. Isto implica que a entrada de um destes dois símbolos acarreta probabilidades iguais de saída de um e de outro, enquanto o terceiro símbolo chega intacto, conforme a Figura 3.3.*a*.

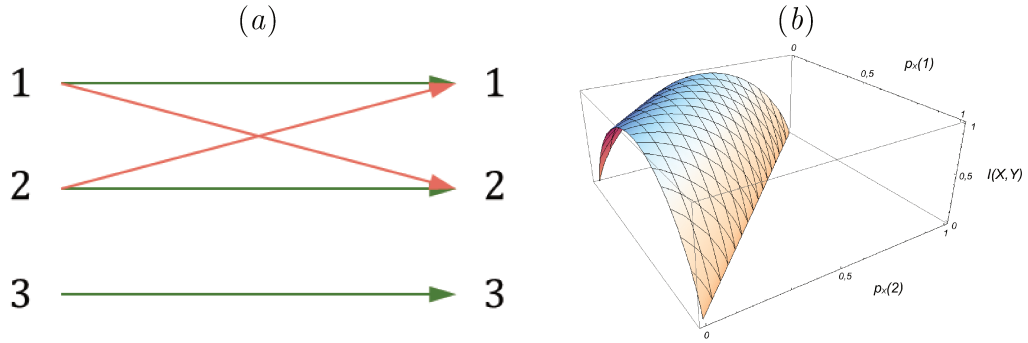


Figura 3.3: (a) Canal defeituoso de três símbolos. A entrada do símbolo 1 ou 2 leva a probabilidades iguais de saída de 1 e 2. A entrada do símbolo 3 leva somente à saída do símbolo 3. (b) Informação mútua em função das probabilidades de uso dos símbolos 1 e 2 (e 3, pois $p_X(1) + p_X(2) + p_X(3) = 1$). A capacidade do canal é o máximo de informação que pode ser transmitida, $C = 1$.

Como calculado no Exemplo 3, o uso único dos símbolos 1 e 2 não permite nenhuma transmissão de informação, assim, se $p_X(3) = 0$ então $I(X,Y) = 0$ bit. Por outro lado, considerando os símbolos 1 e 2 como sendo um mesmo símbolo, recaímos no canal binário sem ruído (Exemplo 2), para o qual a capacidade do canal é $C = 1$ bit e essa taxa máxima de transmissão de informação é atingida quando $p_X(3) = 0,5$, para qualquer combinação entre $p_X(1)$ e $p_X(2)$. Na Figura 3.3.*b* observamos o máximo da informação mútua ao longo da reta $p_X(1) = 0,5 - p_X(2)$ e o mínimo quando $p_X(3) = 0$, na reta $p_X(1) = 1 - p_X(2)$, ou quando $p_X(1) = p_X(2) = 0$.

Capítulo 4

A Luz e Seus Estados

Atualmente, a teoria quântica da radiação eletromagnética é a teoria mais bem sucedida e completa da óptica: jamais suas previsões foram refutadas por experimentos [6]. Neste capítulo faremos a quantização canônica do campo de radiação e apresentaremos os estados de Fock, os estados coerentes e os estados comprimidos da luz.

4.1 A quantização do campo eletromagnético no vácuo

Nesta seção, em concordância com as Equações de Maxwell no Vácuo, definimos o potencial vetor e, utilizando o *Gauge de Coulomb*, obtemos uma equação de onda homogênea [22]. Pela expansão do potencial vetor em termos de ondas planas, obtemos uma equação de oscilador harmônico para cada amplitude de campo [6]. A quantização canônica destes osciladores harmônicos leva aos operadores de criação e aniquilação de fótons do campo luminoso e aos estados de Fock.

4.1.1 Equações de Maxwell no vácuo

$$\nabla \times \vec{E}(\vec{r},t) = -\frac{\partial}{\partial t}\vec{B}(\vec{r},t) \tag{4.1.1}$$

$$\nabla \times \vec{B}(\vec{r},t) = \frac{1}{c^2}\frac{\partial}{\partial t}\vec{E}(\vec{r},t) \tag{4.1.2}$$

$$\nabla \cdot \vec{E}(\vec{r},t) = 0 \tag{4.1.3}$$

$$\nabla \cdot \vec{B}(\vec{r},t) = 0 \tag{4.1.4}$$

4.1.2 Definição dos potenciais vetorial e escalar

Para todo e qualquer campo vetorial $\vec{F}$ temos que $\nabla \cdot \left(\nabla \times \vec{F}\right) = 0$. Como podemos sempre encontrar um campo vetorial $\vec{A}$ que se origine da equação $\nabla \times \nabla \times \vec{A} = \frac{1}{c^2}\frac{\partial}{\partial t}\vec{E}$, e este campo automaticamente irá satisfazer $\nabla \cdot \left(\nabla \times \vec{A}\right) = 0$, podemos defini-lo a partir de

$$\vec{B} = \nabla \times \vec{A} \tag{4.1.5}$$

como se o campo magnético fosse originado por uma entidade mais fundamental, chamada *Potencial Vetor*[1]. Utilizando o potencial vetor na [Eq. 4.1.1] obtemos:

$$\nabla \times \left[\vec{E}(\vec{r},t) + \frac{\partial \vec{A}(\vec{r},t)}{\partial t}\right] = 0$$

Que nos permite escrever:

$$\vec{E}(\vec{r},t) + \frac{\partial \vec{A}(\vec{r},t)}{\partial t} = -\nabla\Phi(\vec{r},t) \tag{4.1.6}$$

Sugerindo que há ainda outro potencial necessário à completa determinação dos campos eletromagnéticos, o chamado *potencial escalar* $\Phi(\vec{r},t)$. Estes potenciais obedecem equações mais simples, possuem menos componentes (apenas quatro ao invés de seis) e carregam todas as informações dos campos $\vec{E}$ e $\vec{B}$, que podem ser recuperados através das equações [Eq. 4.1.5] e [Eq. 4.1.6].

4.1.3 Obtenção de uma equação de onda para o potencial vetor

Tomando o rotacional da [Eq. 4.1.2], o divergente da [Eq. 4.1.6] e utilizando as outras relações, as 4 equações de Maxwell são transformadas em apenas 2:

$$\nabla \times \nabla \times \vec{A}(\vec{r},t) + \frac{1}{c^2}\frac{\partial^2}{\partial t^2}\vec{A}(\vec{r},t) = -\frac{1}{c^2}\frac{\partial}{\partial t}\nabla\Phi(\vec{r},t) \tag{4.1.7}$$

$$\nabla \cdot \nabla\Phi(\vec{r},t) = -\frac{\partial}{\partial t}\nabla \cdot \vec{A}(\vec{r},t) \tag{4.1.8}$$

Estas duas equações diferenciais parciais estão acopladas, mas pode-se demonstrar que há uma infinidade de potenciais $\vec{A}$ e Φ que dão origem aos mesmos campos $\vec{E}$ e $\vec{B}$. Esta liberdade nos permite desacoplar as equações [Eq. 4.1.7] e [Eq. 4.1.8] de diversas maneiras e dá

[1] A descoberta [20] e comprovação [21] do efeito Aharonov-Bohm, em que a função de onda quântica de um elétron é alterada ao atravessar uma região onde $\vec{B} = 0$ mas $\vec{A} \neq 0$, sugere que o campo $\vec{A}$ é de fato mensurável e possui origem física.

origem à escolha do chamado *Gauge* (calibre). Para a quantização do campo eletromagnético utiliza-se o *Gauge de Coulomb*:

$$\nabla \cdot \vec{A}(\vec{r},t) \equiv 0 \tag{4.1.9}$$

e faz-se a expansão $\nabla \times \nabla \times \vec{A} = \nabla\left(\nabla \cdot \vec{A}\right) - \nabla^2 \vec{A}$, isto resulta a equação:

$$\nabla^2 \vec{A}(\vec{r},t) - \frac{1}{c^2}\frac{\partial^2}{\partial t^2}\vec{A}(\vec{r},t) = 0 \tag{4.1.10}$$

que é uma equação de ondas para o potencial vetor.

4.1.4 Expansão em ondas planas

Para simplificar o tratamento, consideramos o campo restrito a um volume cúbico L^3 e expandimos o potencial vetor em termos de ondas planas:

$$\vec{A}(\vec{r},t) = \frac{1}{\varepsilon_0^{1/2} L^{3/2}} \sum_{\vec{k}} \vec{\mathcal{A}}_{\vec{k}}(t)\, e^{i\vec{k}\cdot\vec{r}} \tag{4.1.11}$$

onde $\vec{k} = \left(\frac{2\pi n_1}{L}, \frac{2\pi n_2}{L}, \frac{2\pi n_3}{L}\right)$; $n_1, n_2, n_3 = 0, \pm 1, \pm 2, ...$; a somatória deve ser pensada como sendo sobre os índices n_1, n_2, n_3 e a constante multiplicativa evidenciada será conveniente mais adiante.

Para que a onda seja transversal impomos, para qualquer $\vec{r}$, que $\vec{k} \cdot \vec{A}(\vec{r},t) = 0$, isto implica:

$$\vec{k} \cdot \vec{\mathcal{A}}_{\vec{k}}(t) = 0 \tag{4.1.12}$$

e para que $\vec{A}(\vec{r},t)$ seja real devemos ter

$$\vec{\mathcal{A}}_{\vec{k}}(t) = \vec{\mathcal{A}}^*_{-\vec{k}}(t) \tag{4.1.13}$$

Substituindo esta expansão na equação homogênea para o potencial vetor [Eq. 4.1.10] e requisitando sua validade para qualquer $\vec{r}$ (as ondas planas $e^{i\vec{k}\cdot\vec{r}}$ formam um conjunto linearmente independente) obtemos todo um conjunto de equações:

$$\left(\omega_k^2 + \frac{\partial^2}{\partial t^2}\right) \vec{\mathcal{A}}_{\vec{k}}(t) = 0 \tag{4.1.14}$$

onde foi introduzida convenientemente a frequência angular $\omega_k \equiv ck$. A condição imposta pela [Eq. 4.1.13] nos disponibiliza apenas as soluções do tipo

$$\vec{\mathcal{A}}_{\vec{k}}(t) = \vec{c}_k e^{-i\omega_k t} + \vec{c}^*_{-\vec{k}} e^{i\omega_k t} \tag{4.1.15}$$

4.1.5 Vetores unitários de polarização

Devido à [Eq. 4.1.12], as funções vetoriais $\vec{\mathcal{A}}_{\vec{k}}(t)$ são vetores contidos em um plano perpendicular à direção de propagação $\vec{k}$. Para a representação de vetores neste plano, é conveniente a escolha de uma base constituída de dois vetores unitários e ortogonais $\hat{\varepsilon}_{\vec{k}1}$ e $\hat{\varepsilon}_{\vec{k}2}$ chamados de *vetores unitários de polarização*. As propriedades de transversalidade, ortonormalidade e orientação normal da base são traduzidas matematicamente como:

$$\vec{k}\cdot\vec{\varepsilon}_{\vec{k}s} = 0 \tag{4.1.16}$$

$$\vec{\varepsilon}_{\vec{k}s}\cdot\vec{\varepsilon}_{\vec{k}s'} = \delta_{ss'} \tag{4.1.17}$$

$$\vec{\varepsilon}_{\vec{k}1}\times\vec{\varepsilon}_{\vec{k}2} = \vec{k}/k \tag{4.1.18}$$

com $s, s' = 1, 2$. Estas condições não fixam completamente os vetores de base, que ficam livres para rotacionar em torno de $\vec{k}$ (polarização circular). Neste texto será considerada apenas a resolução da amplitude do campo em termos de polarização linear. O tratamento mais completo pode ser encontrado no livro de Mandel e Wolf [6].

Em termos dos vetores de base temos:

$$\vec{c}_{\vec{k}} = \sum_{s=1}^{2} c_{\vec{k}s}\vec{\varepsilon}_{\vec{k}s} \tag{4.1.19}$$

E a expansão completa do potencial vetor fica:

$$\begin{aligned}
\vec{A}(\vec{r},t) &= \frac{1}{\varepsilon_0^{1/2}L^{3/2}}\sum_{\vec{k}}\sum_{s}\left[c_{\vec{k}s}\vec{\varepsilon}_{\vec{k}s}e^{-i\omega_k t} + c^*_{-\vec{k}s}\vec{\varepsilon}_{-\vec{k}s}e^{i\omega_k t}\right]e^{i\vec{k}\cdot\vec{r}} \\
&= \frac{1}{\varepsilon_0^{1/2}L^{3/2}}\sum_{\vec{k}}\sum_{s}\left[c_{\vec{k}s}\vec{\varepsilon}_{\vec{k}s}e^{i\left(\vec{k}\cdot\vec{r}-\omega_k t\right)} + c^*_{\vec{k}s}\vec{\varepsilon}_{\vec{k}s}e^{-i\left(\vec{k}\cdot\vec{r}-\omega_k t\right)}\right] \\
&= \frac{1}{\varepsilon_0^{1/2}L^{3/2}}\sum_{\vec{k}}\sum_{s}\left[u_{\vec{k}s}(t)\,\vec{\varepsilon}_{\vec{k}s}e^{i\vec{k}\cdot\vec{r}} + u^*_{\vec{k}s}(t)\,\vec{\varepsilon}_{\vec{k}s}e^{-i\vec{k}\cdot\vec{r}}\right]
\end{aligned} \tag{4.1.20}$$

onde aproveitamos que a somatória corre sobre valores positivos e negativos das componentes de $\vec{k}$ para trocar seu sinal no segundo termo da segunda linha e nomeamos:

$$u_{\vec{k}s}(t) = c_{\vec{k}s}e^{-i\omega_k t} \tag{4.1.21}$$

A expansão [Eq. 4.1.20] pode ser vista como uma expansão sobre as funções vetoriais $\vec{\varepsilon}_{\vec{k}s}e^{i\vec{k}\cdot\vec{r}}$ com coeficientes complexos $u_{\vec{k}s}(t)$. Os campos elétrico e magnético são obtidos das

[Eq. 4.1.5] e [Eq. 4.1.6] levando-se em conta o Gauge de Coulomb:

$$\begin{aligned}\vec{E}(\vec{r},t) &= -\frac{\partial \vec{A}(\vec{r},t)}{\partial t} \\ &= \frac{i}{\varepsilon_0^{1/2} L^{3/2}} \sum_{\vec{k}} \sum_{s} \omega_k \left[u_{\vec{k}s}(t)\, \vec{\varepsilon}_{\vec{k}s} e^{i\vec{k}\cdot\vec{r}} - u^*_{\vec{k}s}(t)\, \vec{\varepsilon}_{\vec{k}s} e^{-i\vec{k}\cdot\vec{r}} \right] \end{aligned} \tag{4.1.22}$$

$$\begin{aligned}\vec{B}(\vec{r},t) &= \nabla \times \vec{A}(\vec{r},t) \\ &= \frac{i}{\varepsilon_0^{1/2} L^{3/2}} \sum_{\vec{k}} \sum_{s} \left[u_{\vec{k}s}(t) \left(\vec{k} \times \vec{\varepsilon}_{\vec{k}s} \right) e^{i\vec{k}\cdot\vec{r}} - u^*_{\vec{k}s}(t) \left(\vec{k} \times \vec{\varepsilon}_{\vec{k}s} \right) e^{-i\vec{k}\cdot\vec{r}} \right] \end{aligned} \tag{4.1.23}$$

4.1.6 A energia do campo eletromagnético

A energia clássica contida no campo eletromagnético restrito a um volume L^3 é dada por:

$$\mathcal{H} = \frac{1}{2} \int_{L^3} \left[\varepsilon_0^2 \vec{E}^2(\vec{r},t) + \frac{1}{\mu_0^2} \vec{B}^2(\vec{r},t) \right] \mathrm{d}^3 r \tag{4.1.24}$$

Utilizando as expressões para $\vec{E}(\vec{r},t)$ e $\vec{B}(\vec{r},t)$ e efetuando a integral obtemos:

$$\mathcal{H} = 2 \sum_{\vec{k}} \sum_{s} \omega_k^2 \left| u_{\vec{k}s}(t) \right|^2 \tag{4.1.25}$$

Introduzindo pares de variáveis reais canônicas $q_{\vec{k}s}(t)$ e $p_{\vec{k}s}(t)$ tal que

$$q_{\vec{k}s}(t) = u_{\vec{k}s}(t) + u^*_{\vec{k}s}(t) \tag{4.1.26}$$

$$p_{\vec{k}s}(t) = -i\omega_k \left[u_{\vec{k}s}(t) - u^*_{\vec{k}s}(t) \right] \tag{4.1.27}$$

temos entre elas as relações

$$\begin{aligned}\frac{\partial}{\partial t} q_{\vec{k}s}(t) &= p_{\vec{k}s}(t) \\ \frac{\partial}{\partial t} p_{\vec{k}s}(t) &= -\omega_k^2 q_{\vec{k}s}(t)\end{aligned}$$

e a expressão para a energia se torna:

$$\mathcal{H} = \frac{1}{2} \sum_{\vec{k}} \sum_{s} \left[p^2_{\vec{k}s}(t) + \omega_k^2 q^2_{\vec{k}s}(t) \right] \tag{4.1.28}$$

Em termos destas variáveis o potencial vetor fica:

$$\vec{A}(\vec{r},t)=\frac{1}{2\varepsilon_0^{1/2}L^{3/2}}\sum_{\vec{k}}\sum_{s}\left\{\left[q_{\vec{k}s}\left(t\right)+\frac{i}{\omega_k}p_{\vec{k}s}\left(t\right)\right]\vec{\varepsilon}_{\vec{k}s}e^{i\vec{k}\cdot\vec{r}}+\left[q_{\vec{k}s}\left(t\right)-\frac{i}{\omega_k}p_{\vec{k}s}\left(t\right)\right]\vec{\varepsilon}_{\vec{k}s}e^{-i\vec{k}\cdot\vec{r}}\right\} \tag{4.1.29}$$

4.1.7 A quantização canônica

As previsões da mecânica quântica se reduzem às previsões da mecânica clássica quando as incertezas que acompanham os observáveis são negligíveis. Este fato nos leva a interpretar a mecânica clássica como um caso limite da mecânica quântica. A "generalização" de observáveis clássicos em observáveis quânticos não pode ainda ser feita através de uma técnica geral, válida para *todos* os sistemas dinâmicos. Entretanto, através de uma analogia clássica, esta conversão pode ser feita para uma ampla gama de sistemas. As variáveis canônicas $q_{\vec{k}s}\left(t\right)$ e $p_{\vec{k}s}\left(t\right)$ podem ser convertidas em operadores através das etapas expressas na Seção 21 do compacto e esclarecedor livro de Dirac [24]. No formalismo de Hamilton, algumas quantidades importantes são invariantes por uma mudança do sistema de coordenadas canônico, dentre estes invariantes está os colchetes de Poisson [25]:

$$\left\{u,v\right\}=\sum_{\vec{k},s}\left\{\frac{\partial u}{\partial q_{\vec{k}s}}\frac{\partial v}{\partial p_{\vec{k}s}}-\frac{\partial u}{\partial p_{\vec{k}s}}\frac{\partial v}{\partial q_{\vec{k}s}}\right\} \tag{4.1.30}$$

onde u e v são duas variáveis dinâmicas, funções do conjunto de variáveis canônicas $q_{\vec{k}s}$ e $p_{\vec{k}s}$. Diretamente da definição são obtidas diversas propriedades dos colchetes de Poisson. Introduzimos então os colchetes de Poisson quântico, em analogia ao clássico, e assumimos que este satisfará as mesmas propriedades do clássico. Estas propriedades são suficientes para se determinar a forma dos colchetes de Poisson quântico de quaisquer duas variáveis u e v [24]:

$$\left[\hat{u},\hat{v}\right]=\hat{u}\hat{v}-\hat{v}\hat{u}=i\hbar\left\{u,v\right\} \tag{4.1.31}$$

Onde $\hbar$ foi introduzido como uma constante universal com dimensões de ação e é determinada de forma que a teoria esteja de acordo com os experimentos.

Quando as variáveis dinâmicas u e v são as próprias variáveis canônicas, os colchetes de

Poisson clássicos ficam:

$$\begin{aligned}\left\{q_{\vec{k}s}, q_{\vec{k}'s'}\right\} &= 0\\ \left\{p_{\vec{k}s}, p_{\vec{k}'s'}\right\} &= 0\\ \left\{q_{\vec{k}s}, p_{\vec{k}'s'}\right\} &= \delta_{\vec{k}\vec{k}'}\delta_{ss'}\end{aligned}$$

E temos os colchetes de Poisson quânticos correspondentes:

$$\begin{aligned}\hat{q}_{\vec{k}s}\hat{q}_{\vec{k}'s'} - \hat{q}_{\vec{k}'s'}\hat{q}_{\vec{k}s} &= 0\\ \hat{p}_{\vec{k}s}\hat{p}_{\vec{k}'s'} - \hat{p}_{\vec{k}'s'}\hat{p}_{\vec{k}s} &= 0\\ \hat{q}_{\vec{k}s}\hat{p}_{\vec{k}'s'} - \hat{p}_{\vec{k}'s'}\hat{q}_{\vec{k}s} &= i\hbar\delta_{\vec{k}\vec{k}'}\delta_{ss'}\end{aligned} \tag{4.1.32}$$

Estas expressões são chamadas *relações de comutação* [Eq. 4.1.32] e a partir delas podemos calcular as relações de comutação para outros operadores, correspondentes a variáveis dinâmicas que sejam funções de $q_{\vec{k}s}$ e $p_{\vec{k}s}$[2].

4.2 Os Estados de Fock

Tendo finalmente chegado à mecânica quântica, os autoestados de energia do operador hamiltoniano podem ser encontrados facilmente através de uma "técnica algébrica diabolicamente inteligente" [26]. Definimos dois operadores não hermitianos, compostos a partir dos operadores $\hat{q}_{\vec{k}s}$ e $\hat{p}_{\vec{k}s}$:

$$\hat{a}_{\vec{k}s}(t) = \frac{1}{\sqrt{2\hbar\omega_k}}\left[\omega_k\hat{q}_{\vec{k}s}(t) + i\hat{p}_{\vec{k}s}(t)\right] \tag{4.2.1}$$

$$\hat{a}^{\dagger}_{\vec{k}s}(t) = \frac{1}{\sqrt{2\hbar\omega_k}}\left[\omega_k\hat{q}_{\vec{k}s}(t) - i\hat{p}_{\vec{k}s}(t)\right] \tag{4.2.2}$$

[2]As relações de comutação em um agrupamento de operadores formam um conjunto de regras chamado de álgebra. A álgebra contém todas as informações dos operadores e seu conhecimento permite, por exemplo, obter representações para estes operadores. Exemplos famosos são a álgebra de Weyl-Heisenberg (ou do oscilador harmônico), para os operadores $\left\{A_-, A_+, \hat{1}\right\}$, e a álgebra do momento angular, para os operadores $\{L_-, L_+, L_0\}$.

E encontramos as relações de comutação:

$$\begin{aligned}\left[\hat{a}_{\vec{k}s}, \hat{a}_{\vec{k}'s'}\right] &= 0 \\ \left[\hat{a}^{\dagger}_{\vec{k}s}, \hat{a}^{\dagger}_{\vec{k}'s'}\right] &= 0 \\ \left[\hat{a}_{\vec{k}s}, \hat{a}^{\dagger}_{\vec{k}'s'}\right] &= \delta_{\vec{k}\vec{k}'}\delta_{ss'}\end{aligned} \tag{4.2.3}$$

Utilizando as equações [Eq. 4.2.1],[Eq. 4.2.2] e [Eq. 4.2.3] para escrever o hamiltoniano com ordenamento normal (operadores $\hat{a}^{\dagger}_{\vec{k}s}(t)$ mais à esquerda e operadores $\hat{a}_{\vec{k}s}(t)$ mais à direita), temos:

$$\hat{\mathcal{H}} = \sum_{\vec{k}} \sum_{s} \hbar\omega_k \left[\hat{a}^{\dagger}_{\vec{k}s}(t)\, \hat{a}_{\vec{k}s}(t) + \frac{1}{2}\right] \tag{4.2.4}$$

Desta equação notamos que o operador hamiltoniano é formado por muitas parcelas, cada uma devida a um modo do campo $\vec{k}s$.

A partir deste ponto consideraremos apenas um dos modos do campo e passaremos a ocultar o subscrito $\vec{k}s$. O uso do subscrito será feito em passagens onde a interpretação pode ser errônea.

Entre o operador hamiltoniano e os operadores de criação e aniquilação temos as relações de comutação:

$$\begin{aligned}\left[\hat{\mathcal{H}}, \hat{a}\right] &= -\hbar\omega\hat{a} \\ \left[\hat{\mathcal{H}}, \hat{a}^{\dagger}\right] &= \hbar\omega\hat{a}^{\dagger}\end{aligned}$$

Para os autoestados de energia temos a equação:

$$\hat{\mathcal{H}}\,|E\rangle = E\,|E\rangle$$

Fazemos então a pergunta: Qual seria a energia de um estado $|\psi\rangle = \hat{a}\,|E\rangle$? Vejamos:

$$\hat{\mathcal{H}}\,|\psi\rangle = \hat{\mathcal{H}}\hat{a}\,|E\rangle = \hat{a}\hat{\mathcal{H}}\,|E\rangle + \left[\hat{\mathcal{H}}, \hat{a}\right]|E\rangle = (E - \hbar\omega)\,|\psi\rangle \tag{4.2.5}$$

E a energia de um estado $|\phi\rangle = \hat{a}^{\dagger}\,|E\rangle$?

$$\hat{\mathcal{H}}\,|\phi\rangle = \hat{\mathcal{H}}\hat{a}^{\dagger}\,|E\rangle = \hat{a}^{\dagger}\hat{\mathcal{H}}\,|E\rangle + \left[\hat{\mathcal{H}}, \hat{a}^{\dagger}\right]|E\rangle = (E + \hbar\omega)\,|\phi\rangle \tag{4.2.6}$$

Notamos portanto que os operadores $\hat{a}$ e $\hat{a}^{\dagger}$ retiram ou adicionam uma porção $\hbar\omega$ de energia ao estado da luz. A estes "pacotes" de energia chamamos fótons e os operadores $\hat{a}$

e $\hat{a}^\dagger$ são chamados operadores de *aniquilação* e *criação* de fótons, respectivamente. Estes fótons criados são excitações de um único modo (o modo ao qual o operador $\hat{a}^\dagger_{\vec{k}s}$ se refere).

Matematicamente obtivemos um infinito número de estados, até mesmo estado bastante estranhos com energia negativa. Neste ponto, consideramos nosso conhecimento da natureza e esperamos que haja um estado de energia mínima, que chamaremos *estado de vácuo* $|0\rangle$ e para o qual impomos:

$$\hat{a}\,|0\rangle = 0 \tag{4.2.7}$$

Contra-intuitivamente, a energia desse estado não é nula:

$$\hat{\mathcal{H}}\,|0\rangle = \sum_{\vec{K}s} \frac{1}{2}\hbar\omega_k\,|0\rangle \tag{4.2.8}$$

Esta energia, chamada *energia do vácuo*, dá origem a diversos fenômenos importantes, como o *efeito Casimir* e a *emissão espontânea* de radiação pelos átomos.

Partindo do vácuo, podemos agora "criar" fótons em um determinado modo do campo. Para cada fóton que adicionamos, nomeamos o estado com o número de fótons (daquele modo particular):

$$\left(\hat{a}^\dagger\right)^n |0\rangle \propto |n\rangle \tag{4.2.9}$$

Com um pouco de álgebra, usando-se as relações de comutação, pode-se mostrar que:

$$\hat{a}\,|n\rangle = \sqrt{n}\,|n-1\rangle \tag{4.2.10}$$

$$\hat{a}^\dagger\,|n\rangle = \sqrt{n+1}\,|n+1\rangle \tag{4.2.11}$$

E, após o uso iterativo da segunda equação, obtemos:

$$|n\rangle = \frac{1}{\sqrt{n!}}\left(\hat{a}^\dagger\right)^n |0\rangle \tag{4.2.12}$$

Aqui introduzimos o *operador número de fótons*:

$$\hat{n} = \hat{a}^\dagger\hat{a} \tag{4.2.13}$$

$$\hat{n}\,|n\rangle = n\,|n\rangle \tag{4.2.14}$$

E o operador hamiltoniano fica:

$$\hat{\mathcal{H}} = \sum_{\vec{k}s} \hbar\omega_k \left(\hat{n}_{\vec{k}s} + \frac{1}{2} \right) \tag{4.2.15}$$

A união de todos os operadores número $\hat{n}_{\vec{k}s}$ forma um *conjunto completo de observáveis que comutam*. Isto permite a descrição completa do campo através dos números de ocupação de todos os infinitos modos. O produto direto de todos os estados dos modos forma o chamado *estado de Fock*:

$$|\{n\}\rangle = \prod_{\vec{k}s} \left| \hat{n}_{\vec{k}s} \right\rangle \tag{4.2.16}$$

4.3 Estados Coerentes da Luz[3]

Os estados coerentes foram descobertos pela primeira vez por Schrödinger, em 1926, em conexão com o oscilador harmônico quântico. Por serem estados cujo produto de incertezas é mínimo, permaneceram por muitos anos como uma curiosidade científica. Apenas com os trabalhos de Glauber, entre 1963 e 1965, sua importância e utilidades foram reconhecidas. Glauber cunhou o nome "*coherent states*" e garantiu que estes estados estariam no coração da óptica quântica [6, 11].

A coerência é a propriedade da luz que se traduz em uma manutenção da *incerteza de amplitude* de campo elétrico na ausência de perdas. Desta forma, para um grande *ensemble* de pulsos de luz coerente, a medição do campo elétrico gera uma distribuição gaussiana cuja largura (incerteza) é a mesma para qualquer tempo em que as medidas sejam realizadas, sendo alterada apenas a posição do pico da distribuição (valor médio ou esperado do campo) conforme a Figura 4.1.

Esta característica de coerência é natural em campos da física clássica, onde assume-se que a incerteza não é intrínseca ao próprio campo, mas sim ao procedimento de medida utilizado. Desta forma, o uso de um mesmo procedimento implica em um mesmo desvio, independente do tempo durante o qual o campo evoluiu.

Considerando-se apenas um modo do campo eletromagnético, o estado coerente se origina da equação de autovalores:

$$\hat{a} \left| \alpha \right\rangle = \alpha \left| \alpha \right\rangle \tag{4.3.1}$$

Esta equação nos diz que a remoção de um fóton do estado coerente (para que uma medida seja efetuada, por exemplo) não deve alterar o estado. Na mecânica clássica uma

[3]Nesta seção e nas seguintes será considerado apenas um modo do campo eletromagnético. Esta restrição não implica em perda de generalidade mas simplifica as expressões, graças à remoção dos índices $\vec{k}s$.

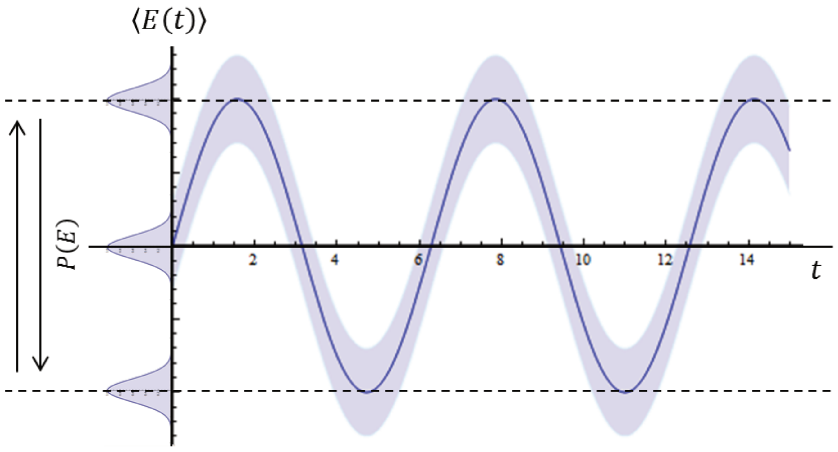


Figura 4.1: Representação da evolução temporal do campo elétrico e sua incerteza para um pulso de luz coerente [5]. A distribuição gaussiana (incerteza) para a detecção do campo elétrico não perde sua forma, apenas oscila entre as máximas amplitudes.

medida pode, em princípio, ser realizada com qualquer precisão e sem alterações no sistema, conforme a tecnologia disponível. Tais propriedades de um sistema clássico são mimetizadas pelos estados coerentes da luz, também chamados *estados clássicos da luz*.

4.3.1 Representação dos estados coerentes da luz em termos dos estados de Fock

Nesta seção, queremos encontrar coeficientes c_n que tornem possível a expansão:

$$|\alpha\rangle = \sum_{n=0}^{\infty} c_n |n\rangle \tag{4.3.2}$$

Para isto, analisamos o efeito de uma aplicação do operador $\hat{a}$:

$$\begin{aligned} \hat{a}|\alpha\rangle &= \hat{a}\sum_{n=0}^{\infty} c_n |n\rangle \\ \alpha|\alpha\rangle &= \sum_{n=1}^{\infty} c_n\sqrt{n}\,|n-1\rangle \end{aligned}$$

Neste ponto, renomeamos o índice da somatória $n = n'+1$ e expandimos o ket à esquerda:

$$\alpha\sum_{n=0}^{\infty} c_n |n\rangle = \sum_{n'=0}^{\infty} c_{n'+1}\sqrt{n'+1}\,|n'\rangle$$

Devido à ortonormalidade dos estados de Fock, a igualdade acima só é verdadeira se

$$c_{n+1}\sqrt{n+1} = \alpha c_n$$

e desta relação de recorrência, obtemos:

$$c_n = \frac{\alpha^n}{\sqrt{n!}} c_0 \tag{4.3.3}$$

O coeficiente c_0 é fixado (a menos de uma fase) através da normalização do estado coerente:

$$\langle \alpha | \alpha \rangle = \sum_{n=0}^{\infty} \sum_{n'=0}^{\infty} \frac{\alpha^n}{\sqrt{n!}} \frac{(\alpha^*)^{n'}}{\sqrt{n'!}} |c_0|^2 \langle n | n' \rangle = \sum_{n=0}^{\infty} \frac{|\alpha|^{2n}}{n!} |c_0|^2 = e^{|\alpha|^2} |c_0|^2$$

$$\begin{aligned} e^{|\alpha|^2} |c_0|^2 &= 1 \\ |c_0| &= e^{-\frac{|\alpha|^2}{2}} \end{aligned} \tag{4.3.4}$$

Finalmente obtemos a expansão:

$$|\alpha\rangle = e^{-\frac{|\alpha|^2}{2}} \sum_{n=0}^{\infty} \frac{\alpha^n}{\sqrt{n!}} |n\rangle \tag{4.3.5}$$

Calculando agora a probabilidade de o estado coerente possuir um fóton no nível n, temos:

$$P(n) = |\langle n | \alpha \rangle|^2 = \frac{|\alpha|^{2n}}{n!} e^{-|\alpha|^2} \tag{4.3.6}$$

E notamos que o estado coerente é uma distribuição de Poisson sobre os estados de Fock. A distribuição de Poisson $P(n) = \frac{\lambda^n}{n!} e^{-\lambda}$ surge como sendo o limite da distribuição binomial $W(n) = \frac{N!}{n!(N-n)!} p^n (1-p)^{N-n}$ para um grande número N de eventos aleatórios, quando a probabilidade p envolvida é muito pequena [27]. Para os estados coerentes, devido à somatória infinita, a probabilidade de ocupação dos níveis deve ser muito pequena para que o número médio de fótons permaneça finito. Para estes estados, o número médio de fótons é $\lambda = \bar{n} = \langle \alpha | \hat{a}^\dagger \hat{a} | \alpha \rangle = |\alpha|^2$.

4.3.2 Os operadores de quadratura do campo

As variáveis conjugadas $\hat{q}$ e $\hat{p}$ possuem diferentes dimensões, sendo útil a definição de novos operadores com uma mesma dimensão:

$$\hat{X} = \frac{1}{2}\left(\hat{a} + \hat{a}^{\dagger}\right) = \sqrt{\frac{\omega}{2\hbar}}\hat{q} \tag{4.3.7}$$

$$\hat{Y} = \frac{1}{2i}\left(\hat{a} - \hat{a}^{\dagger}\right) = \frac{1}{\sqrt{2\hbar\omega}}\hat{p} \tag{4.3.8}$$

Estas definições permitem a representação da distribuição de probabilidades de medida do estado no plano formado pelos eixos X e Y (veja a Figura 4.2.a). Estes eixos são conhecidos como as *quadraturas do campo* e os operadores de quadratura $\hat{X}$ e $\hat{Y}$ são observáveis e mensuráveis, por exemplo, através das técnicas de detecção homódina apresentadas adiante, no Capítulo 5.

4.3.3 O Produto de Incertezas Mínimo

Pode-se mostrar que os estados coerentes são estados cujas incertezas nas variáveis $\hat{q}(t)$ e $\hat{p}(t)$ são constantes no tempo:

$$\left\langle \left(\Delta\hat{q}(t)\right)^2 \right\rangle = \frac{\hbar}{2\omega} \tag{4.3.9}$$

$$\left\langle \left(\Delta\hat{p}(t)\right)^2 \right\rangle = \frac{\hbar\omega}{2} \tag{4.3.10}$$

Delas obtemos o produto de incertezas $\left\langle \left(\Delta\hat{q}\right)^2 \right\rangle \left\langle \left(\Delta\hat{p}\right)^2 \right\rangle = \frac{\hbar^2}{4}$, que é o menor valor permitido pela mecânica quântica.

Notemos agora que as incertezas nas variáveis $\hat{q}(t)$ e $\hat{p}(t)$ são responsáveis pela aparência dos estados na representação de quadraturas, pois:

$$\left\langle \left(\Delta\hat{X}\right)^2 \right\rangle = \frac{\omega}{2\hbar}\left\langle \left(\Delta\hat{q}\right)^2 \right\rangle \tag{4.3.11}$$

$$\left\langle \left(\Delta\hat{Y}\right)^2 \right\rangle = \frac{1}{2\hbar\omega}\left\langle \left(\Delta\hat{p}\right)^2 \right\rangle \tag{4.3.12}$$

Para um estado coerente temos $\left\langle \left(\Delta\hat{X}\right)^2 \right\rangle = \left\langle \left(\Delta\hat{Y}\right)^2 \right\rangle = \frac{1}{4}$, o que implica que sua forma, quando representado no plano das quadraturas, seja circular.

4.3.4 O Operador Deslocamento de Glauber

Verifiquemos o efeito de um operador

$$\hat{D}(\beta) = e^{\beta\hat{a}^\dagger - \beta^*\hat{a}} \tag{4.3.13}$$

sobre um estado de vácuo $|0\rangle$. Usando o teorema de Campbell-Baker-Hausdorff (veja o Apêndice A.2) temos:

$$\begin{aligned}
\hat{D}(\beta)|0\rangle &= e^{\beta\hat{a}^\dagger - \beta^*\hat{a}}|0\rangle \\
&= e^{-\frac{|\beta|^2}{2}} e^{\beta\hat{a}^\dagger} e^{\beta^*\hat{a}}|0\rangle \\
&= e^{-\frac{|\beta|^2}{2}} e^{\beta\hat{a}^\dagger}|0\rangle \\
&= e^{-\frac{|\beta|^2}{2}} \sum_{n=0}^{\infty} \frac{1}{n!}\left(\beta\hat{a}^\dagger\right)^n |0\rangle \\
&= e^{-\frac{|\beta|^2}{2}} \sum_{n=0}^{\infty} \frac{\beta^n}{\sqrt{n!}}|n\rangle \\
\hat{D}(\beta)|0\rangle &= |\beta\rangle
\end{aligned} \tag{4.3.14}$$

Onde usamos a [Eq. 4.2.10] e a expansão de um operador $e^{\hat{A}}$ em série de potências. Notamos que o operador deslocamento de Glauber $\hat{D}(\beta)$ transforma um estado de vácuo em um estado coerente de amplitude β.

Verifiquemos agora o efeito do operador $\hat{D}(\beta)$ sobre um estado coerente $|\alpha\rangle$. Utilizando novamente o teorema de Campbell-Baker-Hausdorff:

$$\begin{aligned}
\hat{D}(\beta)|\alpha\rangle &= \hat{D}(\beta)\hat{D}(\alpha)|0\rangle \\
&= e^{\beta\hat{a}^\dagger - \beta^*\hat{a}} e^{\alpha\hat{a}^\dagger - \alpha^*\hat{a}}|0\rangle \\
&= e^{\frac{1}{2}(\beta\alpha^* - \beta^*\alpha)} e^{(\beta+\alpha)\hat{a}^\dagger - (\beta+\alpha)^*\hat{a}}|0\rangle \\
&= e^{\frac{1}{2}(\beta\alpha^* - \beta^*\alpha)}|\beta+\alpha\rangle
\end{aligned} \tag{4.3.15}$$

E notamos que o deslocamento de um estado coerente leva a outro estado coerente. O significado das [Eq. 4.3.14] e [Eq. 4.3.15] pode ser visualizado no plano das quadraturas do campo, na Figura 4.2.

O operador deslocamento transforma os operadores de amplitude do campo de forma que:

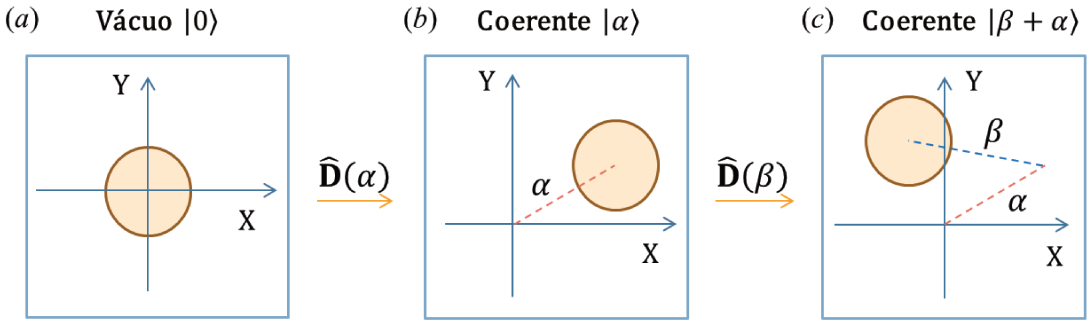


Figura 4.2: (a) Representação de um estado de vácuo $|0\rangle$ no plano das quadraturas do campo. (b) Efeito do efeito do Operador Deslocamento de Glauber sobre o estado de vácuo, e (c) deslocamento do estado coerente de amplitude α para $\alpha + \beta$.

$$\hat{D}(\alpha)^{-1}\hat{a}\hat{D}(\alpha) = \hat{a} + \alpha \tag{4.3.16}$$

$$\hat{D}(\alpha)^{-1}\hat{a}^{\dagger}\hat{D}(\alpha) = \hat{a}^{\dagger} + \alpha^{*} \tag{4.3.17}$$

A união de todos os operadores deslocamento forma um conjunto completo de operadores, desta forma, podemos expressar qualquer operador em termos destes [12].

4.3.5 A Não-Ortogonalidade Dos Estados Coerentes

Utilizando a [Eq. 4.3.15], podemos deduzir que dois estados coerentes não são ortogonais entre si:

$$\begin{aligned}
\langle\alpha|\beta\rangle &= \left[\hat{D}(\alpha)|0\rangle\right]^{*}|\beta\rangle \\
&= \langle 0|\hat{D}(\alpha)^{\dagger}|\beta\rangle \\
&= \langle 0|\hat{D}(-\alpha)|\beta\rangle \\
&= \langle 0|\beta-\alpha\rangle\, e^{\frac{1}{2}(\alpha^{*}\beta-\alpha\beta^{*})} \\
&= e^{-\frac{1}{2}\left(|\beta-\alpha|^{2}+\alpha\beta^{*}-\alpha^{*}\beta\right)} \\
&= e^{\left(-\frac{1}{2}|\alpha|^{2}+\alpha^{*}\beta-\frac{1}{2}|\beta|^{2}\right)}
\end{aligned} \tag{4.3.18}$$

mesmo assim, pode-se mostrar que os estados coerentes satisfazem uma *relação de completeza*:

$$\sum_{n=0}^{\infty} |n\rangle \langle n| = \frac{1}{\pi} \int |\alpha\rangle \langle \alpha| \, \mathrm{d}^2\alpha = 1 \tag{4.3.19}$$

e isto, juntamente com o produto escalar entre estados coerentes, nos permite notar que qualquer estado coerente pode ser escrito em termos dos outros, ou seja, o conjunto dos estados coerentes é *supercompleto* [10].

4.4 Estados Comprimidos da Luz

O princípio da incerteza não impõe restrições sobre a incerteza de cada variável isolada, $\left\langle (\Delta\hat{q})^2 \right\rangle$ ou $\left\langle (\Delta\hat{p})^2 \right\rangle$, mas apenas sobre o seu produto $\left\langle (\Delta\hat{q})^2 \right\rangle \left\langle (\Delta\hat{p})^2 \right\rangle \geqslant \frac{\hbar^2}{4}$. Isto nos dá a liberdade de especular sobre a existência de estados de mínima incerteza em que uma das variáveis, ou quadratura, possui uma incerteza menor que aquela do estado coerente.

Tais estados existem de fato e são factíveis em laboratório. Seu uso nas tecnologias futuras tem sido ampliado a cada dia, graças à descoberta de novas técnicas de preparação, novas aplicações e novas vantagens de uso. Estes estados são os chamados *Estados Comprimidos do Campo Eletromagnético* [7].

4.4.1 A Transformação de Compressão

Respeitando o produto $\left\langle \left(\Delta\hat{X}\right)^2 \right\rangle \left\langle \left(\Delta\hat{Y}\right)^2 \right\rangle \geqslant \frac{1}{16}$, procuramos um estado em que

$$\left\langle \left(\Delta\hat{X}\right)^2 \right\rangle = \frac{1}{4} e^{-2s} \tag{4.4.1}$$

$$\left\langle \left(\Delta\hat{Y}\right)^2 \right\rangle = \frac{1}{4} e^{2s} \tag{4.4.2}$$

com $s \in \mathbb{R}^+$, de forma que estas expressões retornem ao caso coerente quando o *parâmetro de compressão* for $s = 0$. Estas incertezas podem ser obtidas através das simples transformações:

$$\hat{X}_S = \hat{X} e^{-s} \tag{4.4.3}$$

$$\hat{Y}_S = \hat{Y} e^{s} \tag{4.4.4}$$

Destas transformações e das definições [Eq. 4.3.7] e [Eq. 4.3.8] encontramos, com um pouco de álgebra, novos operadores de criação e aniquilação:

$$\hat{a}_S = \hat{a}\cosh s - \hat{a}^\dagger \sinh s \tag{4.4.5}$$
$$\hat{a}_S^\dagger = \hat{a}^\dagger \cosh s - \hat{a}\sinh s \tag{4.4.6}$$

4.4.2 O Operador de *Squeezing*

Procuramos, nesta seção, um operador unitário $\hat{S}(s)$ que realize a transformação de compressão apresentada na seção anterior:

$$\begin{aligned} \hat{S}(s)^{-1}\hat{a}\hat{S}(s) &= \hat{a}_S = \hat{a}\cosh s - \hat{a}^\dagger \sinh s \\ \hat{S}(s)^{-1}\hat{a}^\dagger\hat{S}(s) &= \hat{a}_S^\dagger = \hat{a}^\dagger \cosh s - \hat{a}\sinh s \end{aligned}$$

Partindo da primeira equação, fazendo a expansão em série de Taylor das funções hiperbólicas e reagrupando todos os termos:

$$\begin{aligned} \hat{S}(s)^{-1}\hat{a}\hat{S}(s) &= \hat{a}\left(1+\frac{s^2}{2!}+\frac{s^4}{4!}+...\right) - \hat{a}^\dagger\left(s+\frac{s^3}{3!}+\frac{s^5}{5!}+...\right) \\ &= \hat{a} + (-s)\hat{a}^\dagger + \frac{(-s)^2}{2}\hat{a} + \frac{(-s)^3}{3!} + ... \end{aligned}$$

Notamos que o lado direito da [Eq. 4.4.5] é, na realidade, uma expansão em série de um operador. De acordo com o Apêndice A.1, temos:

$$e^{x\hat{A}}\hat{B}e^{-x\hat{A}} = \hat{B} + x\left[\hat{A},\hat{B}\right] + \frac{x^2}{2}\left[\hat{A},\left[\hat{A},\hat{B}\right]\right] + \frac{x^3}{3!}\left[\hat{A},\left[\hat{A},\left[\hat{A},\hat{B}\right]\right]\right] + ...$$

Por comparação renomeamos $x = -s$ e $\hat{B} = \hat{a}$. Nos resta agora determinar o operador $\hat{A}$, de forma que $\left[\hat{A},\hat{a}\right] = \hat{a}^\dagger$ e $\left[\hat{A},\hat{a}^\dagger\right] = \hat{a}$.

Após alguns cálculos descobrimos que $\hat{A} = \frac{1}{2}\left(\hat{a}^2 - \hat{a}^{\dagger 2}\right)$, e encontramos:

$$\hat{S}(s)^{-1}\hat{a}\hat{S}(s) = e^{-\frac{s}{2}\left(\hat{a}^2-\hat{a}^{\dagger 2}\right)}\hat{a}e^{\frac{s}{2}\left(\hat{a}^2-\hat{a}^{\dagger 2}\right)} \tag{4.4.7}$$

Lembrando que $\hat{S}(s)^{-1} = \hat{S}(s)^\dagger$ (unitário), finalmente identificamos:

$$\hat{S}(s) = e^{\frac{s}{2}\left(\hat{a}^2-\hat{a}^{\dagger 2}\right)} \tag{4.4.8}$$

O *operador de Squeezing* acima realiza uma compressão na direção da quadratura X, reduzindo a incerteza nesta quadratura e "alongando" a incerteza da quadratura Y.

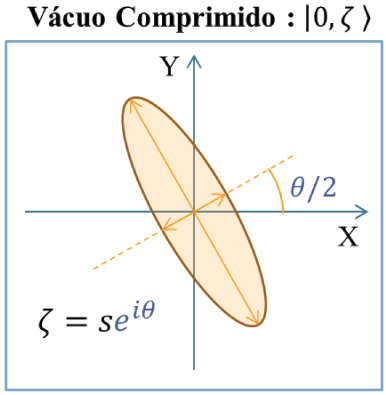


Figura 4.3: Operação de compressão realizada pelo operador $\hat{S}\left(se^{i\theta}\right)$. A compressão ocorre ao longo de um eixo girado de $\theta/2$ em relação à quadratura X.

A compressão ao longo de qualquer direção pode ser feita pelo operador mais geral:

$$\hat{S}(\zeta) = e^{\frac{1}{2}\left(\zeta^* \hat{a}^2 - \zeta \hat{a}^{\dagger 2}\right)} \tag{4.4.9}$$

$$\zeta = se^{i\theta},\ 0 \leqslant s < \infty,\ 0 \leqslant \theta \leqslant 2\pi$$

Que transforma os operadores de criação e aniquilação como:

$$\hat{S}(\zeta)^{-1}\, \hat{a} \hat{S}(\zeta) = \hat{a} \cosh s - \hat{a}^{\dagger} e^{i\theta} \sinh s \tag{4.4.10}$$

$$\hat{S}(\zeta)^{-1}\, \hat{a}^{\dagger} \hat{S}(\zeta) = \hat{a}^{\dagger} \cosh s - \hat{a} e^{-i\theta} \sinh s \tag{4.4.11}$$

e pode-se mostrar que esta compressão ocorre ao longo de um eixo com inclinação $\theta/2$ em relação ao eixo da quadratura X, como representado na Figura 4.3.

4.4.3 Estados Coerentes Comprimidos

A obtenção de um *estado coerente comprimido* pode ser feita de duas maneiras: através de compressão e deslocamento do vácuo (notação de Caves) ou através de deslocamento e compressão do vácuo (notação de Yuen). A não comutabilidade dos operadores $\hat{D}(\alpha)$ e $\hat{S}(\zeta)$ implica que a ordem de aplicação dessas transformações leva a estados finais bastante diferentes [7]. Com o objetivo de se obter o mesmo estado final, precisamos realizar deslocamentos diferentes, como representado na Figura 4.4.

Pode-se mostrar que os parâmetros da notação de Yuen estão relacionados com a notação

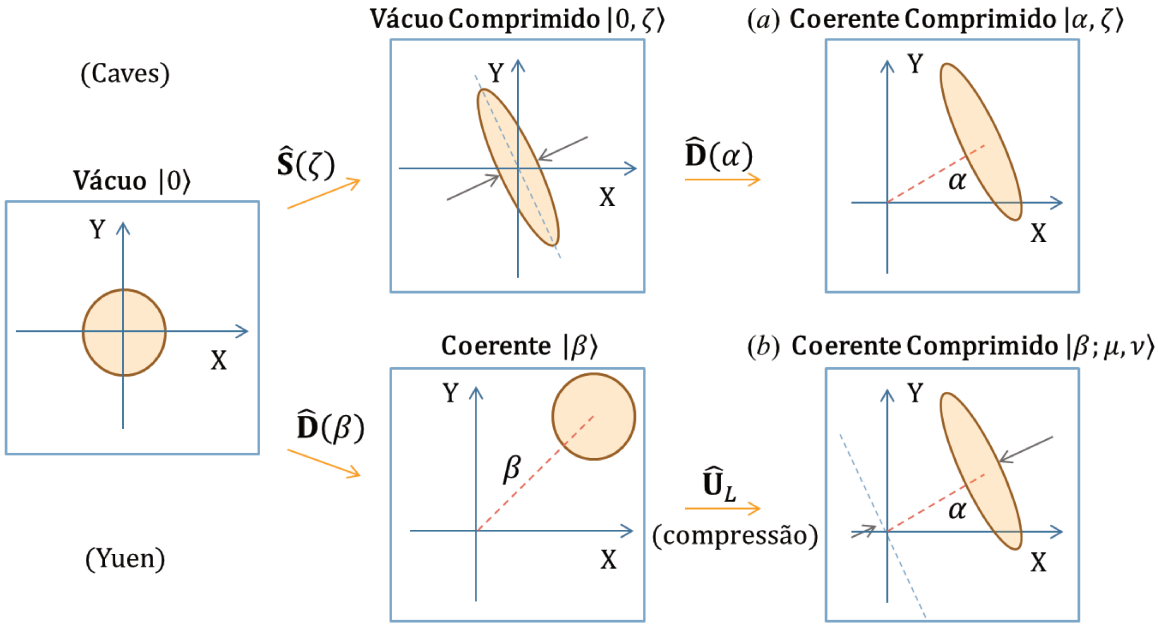


Figura 4.4: (a) Vácuo comprimido e deslocado. (b) Vácuo deslocado e comprimido. A ordem de aplicação dos operadores deslocamento $\hat{D}$ e compressão $\hat{S}$ (e $\hat{U}_L$) só leva aos mesmos estados finais com um fino ajuste dos parâmetros. A razão para isto é que a compressão também "arrasta" o estado de encontro ao eixo de compressão.

de Caves através das expressões:

$$\begin{aligned} \beta &= \mu\alpha + \nu\alpha^* \\ \mu &= \cosh s \\ \nu &= e^{i\theta}\sinh s \end{aligned} \tag{4.4.12}$$

Neste texto será usada a notação de Caves

$$|\alpha,\zeta\rangle = \hat{D}(\alpha)\,\hat{S}(\zeta)\,|0\rangle \tag{4.4.13}$$

Notemos agora que $\hat{D}(-\alpha) = \hat{D}(\alpha)^\dagger$ e $\hat{S}(-\zeta) = \hat{S}(\zeta)^\dagger$. Podemos usar este fato para a obtenção de uma equação de autovalores para um estado coerente comprimido (observando ainda que os operadores são unitários):

$$\begin{aligned} \hat{a}\,|0\rangle &= 0 \\ \hat{D}(\alpha)\,\hat{S}(\zeta)\,\hat{a}\,|0\rangle &= 0 \\ \hat{D}(\alpha)\,\hat{S}(\zeta)\,\hat{a}\hat{S}(\zeta)^\dagger\,\hat{D}(\alpha)^\dagger\,\hat{D}(\alpha)\,\hat{S}(\zeta)\,|0\rangle &= 0 \\ \hat{D}(-\alpha)^\dagger\,\hat{S}(-\zeta)^\dagger\,\hat{a}\hat{S}(-\zeta)\,\hat{D}(-\alpha)\,|\alpha,\zeta\rangle &= 0 \\ \hat{D}(-\alpha)^\dagger\left[\hat{a}\cosh(-s) - \hat{a}^\dagger e^{i\theta}\sinh(-s)\right]\hat{D}(-\alpha)\,|\alpha,\zeta\rangle &= 0 \\ \left[(\hat{a}-\alpha)\cosh s + \left(\hat{a}^\dagger - \alpha^*\right)e^{i\theta}\sinh s\right]|\alpha,\zeta\rangle &= 0 \end{aligned}$$

Onde usamos as [Eq. 4.4.10] e [Eq. 4.4.11], [Eq. 4.3.16] e [Eq. 4.3.17]. Reorganizando os termos, temos:

$$\left(\hat{a}\cosh s + \hat{a}^\dagger e^{i\theta}\sinh s\right)|\alpha,\zeta\rangle = \left(\alpha\cosh s + \alpha^* e^{i\theta}\sinh s\right)|\alpha,\zeta\rangle \tag{4.4.14}$$

Capítulo 5

A Detecção Homódina

O uso de fotodetectores permite apenas uma medida do número médio de fótons e de *momentos de ordem superior*[1]. Estas medidas de intensidade não permitem identificar compressão no campo luminoso, pois não são sensíveis à fase do campo. A detecção de estados comprimidos requer um esquema de medição sensível à fase do campo e capaz de realizar medições da variância de sua quadratura. Um exemplo de esquema de medição capaz de realizar tais medidas é o esquema de detecção homódina [10]. Os protocolos de criptografia com estados contínuos da luz apresentados neste trabalho estão baseados no uso da detecção homódina, por parte de Bob, para a obtenção de dados clássicos dos sinais quânticos enviados por Alice.

5.1 Detecção Homódina Ordinária

No esquema de detecção homódina ordinária, a detecção do sinal é feita pela sua combinação com um campo coerente de grande amplitude e com a mesma frequência. Tal campo pode ser produzido e transmitido paralelamente ao sinal, para se facilitar a manutenção da mesma frequência, ou pode ser produzido diretamente no local de medição, razão pela qual é chamado de *Oscilador Local*. A combinação do sinal com o oscilador local é feita na hora da medição através de um divisor de feixes com uma taxa de reflexão muito pequena (veja a Figura 5.1). A fase existente entre o sinal transmitido e o oscilador local é um parâmetro ajustável experimentalmente e permite medições de quadratura análogas a cortes tomográficos, como será apresentado a seguir.

Fazemos a descrição dos campos envolvidos através de seus operadores de amplitude: $\hat{a}$ para um modo do sinal recebido, $\hat{b}$ para um modo do oscilador local, $\hat{c}$ para um modo do

[1] A dispersão $\overline{(\Delta n)^2}$ do número de fótons é o segundo momento do número de fótons ao redor do número médio de fótons. O conhecimento de todos os momentos de uma distribuição permite, a princípio, a reconstrução de toda a distribuição.

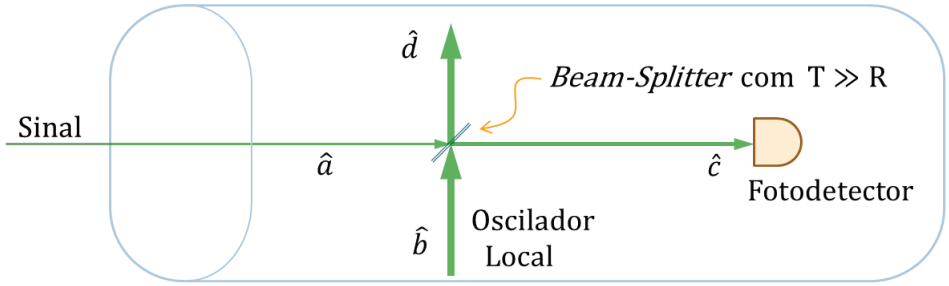


Figura 5.1: Esquema de detecção homódina ordinária. O sinal recebido é combinado, através de um divisor de feixes, com o oscilador local.

campo recebido pelo fotodetector e $\hat{d}$ para um modo do campo restante.

A relação entre os campos de entrada e saída do divisor de feixes pode ser expressa através de seus operadores de amplitude a partir das expressões:

$$\begin{aligned} \hat{c} &= T\hat{a} + R\hat{b} \\ \hat{d} &= -R\hat{a} + T\hat{b} \end{aligned} \tag{5.1.1}$$

Onde R e T são valores reais para a refletância e a transmitância do divisor de feixes ($R^2 + T^2 = 1$) e o sinal negativo na segunda linha se deve ao deslocamento de fase de $\pi/2$ existente entre os campos refletidos e transmitidos para um divisor de feixes simétrico.

No fotodetector o operador número de fótons é dado por:

$$\hat{n}_c = \hat{c}^\dagger \hat{c} = T^2 \hat{a}^\dagger \hat{a} + R^2 \hat{b}^\dagger \hat{b} + RT(\hat{a}^\dagger \hat{b} + \hat{b}^\dagger \hat{a}) \tag{5.1.2}$$

Nestas expressões os operadores não possuem dependência temporal devido ao fato de o sinal recebido e o oscilador local possuírem a mesma frequência.

Estando o oscilador local em um modo excitado como estado coerente com grande amplitude $|\beta_{ol}|$ e fase ϕ_{ol} (relativa à fase do sinal) temos:

$$\hat{b}\,|\beta_{ol}\rangle = |\beta_{ol}|\, e^{i\phi_{ol}}\, |\beta_{ol}\rangle$$

Calculando-se o número médio de fótons no fotodetector através do estado $|\alpha\rangle \otimes |\beta_{ol}\rangle$ e fazendo uma pequena manipulação algébrica encontramos:

$$\langle \hat{n}_c \rangle = T^2 \left\langle \hat{a}^\dagger \hat{a} \right\rangle + R^2 \left|\beta_{ol}\right|^2 + 2RT \left|\beta_{ol}\right| \cdot \left\langle \frac{1}{2} \left(\hat{a}^\dagger e^{i\phi_{ol}} + \hat{a} e^{-i\phi_{ol}} \right) \right\rangle \tag{5.1.3}$$

Sendo $|\beta_{ol}|$ muito grande, o primeiro termo nesta expressão é desprezível em relação aos outros dois. O segundo termo é bem conhecido e pode ser descontado da medição. O terceiro

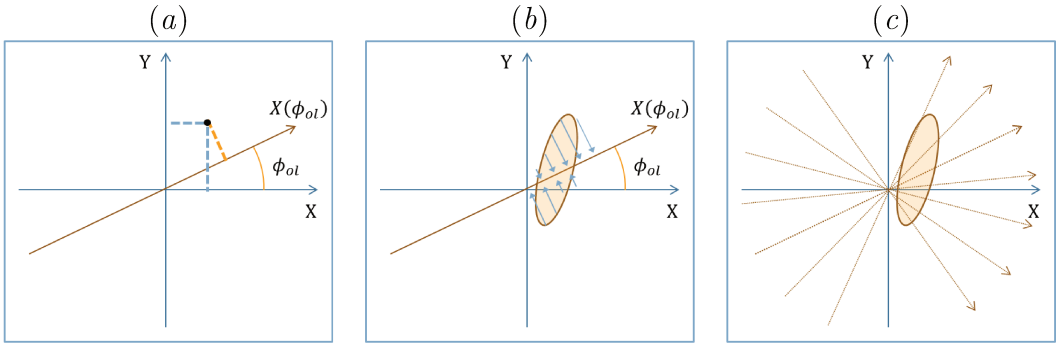


Figura 5.2: (a) Representação do operador de quadratura $\hat{X}(\phi_{ol})$. (b) O estado é projetado sobre o eixo $\hat{X}(\phi_{ol})$ dando origem a uma distribuição de probabilidades. (c) O parâmetro ϕ_{ol} é regulado por Bob, permitindo medições em "cortes tomográficos" da quadratura do campo.

termo, por outro lado, contém um operador semelhante a um operador de quadratura que chamaremos convenientemente de $\hat{X}(\phi_{ol})$. Utilizando a definição $\hat{a} = \hat{X} + i\hat{Y}$ e após alguma manipulação descobrimos o significado deste operador de quadratura:

$$\begin{aligned} \hat{X}(\phi_{ol}) &= \frac{1}{2}\left(\hat{a}^{\dagger}e^{i\phi_{ol}} + \hat{a}e^{-i\phi_{ol}}\right) \\ &= \frac{1}{2}\left[\hat{X}\left(e^{i\phi_{ol}} + e^{-i\phi_{ol}}\right) - i\hat{Y}\left(e^{i\phi_{ol}} - e^{-i\phi_{ol}}\right)\right] \\ &= \hat{X}\cos\phi_{ol} + \hat{Y}\sin\phi_{ol} \end{aligned} \tag{5.1.4}$$

Como representado na Figura 5.2, notamos que o operador de quadratura $\hat{X}(\phi_{ol})$ corresponde simplesmente a uma medição de quadratura sobre um eixo rotacionado de ϕ_{ol} radianos em torno da origem do plano das quadraturas do campo. Desta forma, fica evidente que o esquema de detecção homódina ordinária permite o uso de um simples fotodetector para a obtenção de informações de fase e compressão do campo recebido, sendo mesmo possível a reconstrução completa do estado após uma grande série de medições ("tomografia" - Figura 5.2 (c)).

5.2 Detecção Homódina Balanceada

No esquema anterior, embora $R \ll 1$ (o que implica também em pouca reflexão do ruído que acompanha o oscilador local), quando o sinal é demasiadamente fraco ou o ruído é forte, a medição é prejudicada. Por este motivo é vantajoso o uso de uma pequena modificação neste esquema. Na detecção homódina *balanceada*, o divisor de feixes tem taxas de reflexão e transmissão iguais ($R = T$). A medição é feita por dois detectores, um em cada saída do

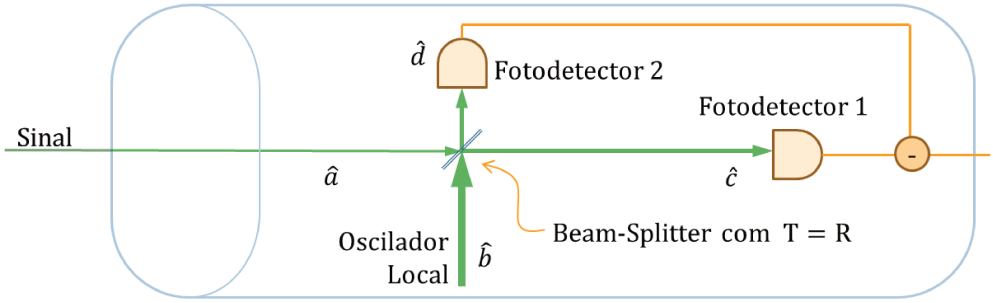


Figura 5.3: Esquema de detecção homódina balanceada. Um divisor de feixes com $R = T$ combina os campos e a medição é feita em ambas as saídas. Os sinais medidos pelos fotodetectores são subtraídos, resultando em uma medida mais limpa de ruídos.

divisor de feixes (veja Figura 5.3). Neste caso, a contribuição do oscilador local (e do ruído) para os sinais medidos pelos fotodetectores pode ser removida através de uma subtração entre os sinais.

O operador número de fótons no fotodetector 1 é dado pela [Eq. 5.1.2], já no fotodetector 2 o número de fótons é $\hat{n}_d = \hat{d}^\dagger \hat{d}$. Lembrando que $R = T = 1/\sqrt{2}$ temos:

$$\hat{n}_c = \frac{1}{2}\hat{a}^\dagger\hat{a} + \frac{1}{2}\hat{b}^\dagger\hat{b} + \frac{1}{2}\left(\hat{a}^\dagger\hat{b} + \hat{b}^\dagger\hat{a}\right) \tag{5.2.1}$$

e

$$\begin{aligned}\hat{n}_d &= R^2\hat{a}^\dagger\hat{a} + T^2\hat{b}^\dagger\hat{b} - RT\left(\hat{a}^\dagger\hat{b} + \hat{b}^\dagger\hat{a}\right) \\ &= \frac{1}{2}\hat{a}^\dagger\hat{a} + \frac{1}{2}\hat{b}^\dagger\hat{b} - \frac{1}{2}\left(\hat{a}^\dagger\hat{b} + \hat{b}^\dagger\hat{a}\right)\end{aligned} \tag{5.2.2}$$

Com uma combinação dos sinais de saída dos fotodetectores, subtraindo a [Eq. 5.2.2] da [Eq. 5.2.1], obtemos:

$$\hat{n}_c - \hat{n}_d = \hat{a}^\dagger\hat{b} + \hat{b}^\dagger\hat{a} \tag{5.2.3}$$

E a medição dessa combinação resulta:

$$\langle\hat{n}_c - \hat{n}_d\rangle = \left\langle\hat{a}^\dagger\hat{b} + \hat{b}^\dagger\hat{a}\right\rangle = 2\left|\beta_{ol}\right|\left\langle\frac{1}{2}\left(\hat{a}^\dagger e^{i\phi_{ol}} + \hat{a}e^{-i\phi_{ol}}\right)\right\rangle = 2\left|\beta_{ol}\right|\left\langle\hat{X}\left(\phi_{ol}\right)\right\rangle \tag{5.2.4}$$

Através da detecção homódina balanceada, o ruído do oscilador local é completamente eliminado, permitindo o uso de um oscilador local mais forte.

Capítulo 6

A Função de Wigner

Graças a *Max Born (1882-1970)*, hoje interpretamos a mecânica quântica como uma teoria estatística. Suas previsões para uma partícula são probabilísticas e só podem ser relacionadas com a mecânica clássica através das probabilidades geradas por um *ensemble* de partículas clássicas. O estudo e descrição clássicos de um tal *ensemble* podem ser bem empreendidos através do uso de conceitos da mecânica estatística e, em particular, da equação de Liouville para distribuições no espaço de fases. Assim, objetivando relacionar a teoria quântica com a clássica, somos levados a procurar uma descrição da mecânica quântica dentro do espaço de fases, evidenciando as conexões existentes entre elas, bem como suas desavenças. Entretanto, devido à incerteza no conhecimento conjunto do momento e posição de uma partícula, não podemos associar diretamente a configuração de um dado sistema quântico com um ponto único no espaço de fases. Esta limitação, intrínseca à mecânica quântica, implica que não é possível a obtenção de uma distribuição *única e verdadeira* de probabilidades, sobre o espaço de fases, para as possíveis configurações deste sistema quântico, mas apenas funções com algumas das propriedades destas distribuições verdadeiras.

Várias destas distribuições foram formuladas com o passar do tempo, cada uma conveniente para o estudo de um dado problema. Neste capítulo apresentaremos uma descrição do operador densidade em termos de uma função real de distribuição sobre as coordenadas do espaço de fases conhecida como *Função de Distribuição de Quasi-Probabilidade de Wigner*, introduzida por *Eugene Paul Wigner (1902-1995)* em 1932 [15, 14, 43]. Mais adiante usaremos a função de Wigner como base para o estudo de dois protocolos de variáveis contínuas, extraindo dela interpretações e distribuições de probabilidades de detecção dos estados transmitidos durante a QKD.

6.1 A Função Característica

Diversas fórmulas para a função de Wigner foram derivadas independentemente em diferentes contextos. Aqui obteremos a função de Wigner como uma transformada de Fourier complexa da função característica, que agora discutiremos.

A expansão de um operador qualquer $\hat{F}$ em termos de produtos de operadores de criação e aniquilação $\hat{a}$ e $\hat{a}^\dagger$ é de grande utilidade para o estudo de osciladores harmônicos e campos quantizados, mas não é univocamente definida. A não comutatividade destes dois operadores dá origem ao problema do ordenamento destes operadores nos produtos, permitindo uma infinidade de expansões ordenadas. Em pouco tempo, descobriu-se que esta indeterminação no ordenamento não se tratava de uma inconveniência, pois a cada tipo de medida corresponde um ordenamento mais apropriado para sua descrição. Neste texto abordaremos o ordenamento simétrico, também conhecido como *ordenamento de Weyl*. Neste ordenamento, cada parcela da expansão será escrita como uma combinação simétrica dos operadores $\hat{a}$ e $\hat{a}^\dagger$ [12]. Introduzimos o conceito de combinação simétrica e sua notação através de dois exemplos:

$$\left\{\left(\hat{a}^\dagger\right)\hat{a}\right\}_{s=0} = \frac{1}{2}\left(\hat{a}^\dagger\hat{a} + \hat{a}\hat{a}^\dagger\right) \tag{6.1.1}$$

$$\left\{\left(\hat{a}^\dagger\right)\hat{a}^2\right\}_{s=0} = \frac{1}{3}\left(\hat{a}^\dagger\hat{a}^2 + \hat{a}\hat{a}^\dagger\hat{a} + \hat{a}^2\hat{a}^\dagger\right) \tag{6.1.2}$$

onde $s = 0$ indica ordenamento simétrico. Outros dois ordenamentos muito úteis são o *ordenamento normal* $\left\{\left(\hat{a}^\dagger\right)^n\hat{a}^m\right\}_{s=1} = \hat{a}^{\dagger n}\hat{a}^m$ e o *antinormal* $\left\{\left(\hat{a}^\dagger\right)^n\hat{a}^m\right\}_{s=-1} = \hat{a}^m\hat{a}^{\dagger n}$.

Como a união de todos os operadores deslocamento forma um conjunto completo de operadores, podemos expandir um operador qualquer $\hat{F}$ como:

$$\hat{F} = \int f(\xi)\,\hat{D}^{-1}(\xi)\,\pi^{-1}\mathrm{d}^2\xi \tag{6.1.3}$$

onde as funções peso são dadas por

$$f(\xi) = \mathbf{Tr}\left[\hat{F}\hat{D}(\xi)\right] \tag{6.1.4}$$

e $\hat{D}(\xi)$ possui ordenamento simétrico:

$$\hat{D}(\xi) = e^{\xi\hat{a}^\dagger - \xi^*\hat{a}} = \sum_{n=0}^{\infty}\frac{1}{n!}\left(\xi\hat{a}^\dagger - \xi^*\hat{a}\right)^n = \sum_{n,m=0}^{\infty}\frac{\xi^n\left(-\xi^*\right)^m}{n!m!}\left\{\left(\hat{a}^\dagger\right)^n\hat{a}^m\right\}_{s=0} \tag{6.1.5}$$

As funções peso aqui definidas são unívocas e quadrado-integráveis. Fazendo esta expansão para o operador densidade obtemos:

$$\hat{\rho} = \frac{1}{\pi} \int \chi(\xi)\, \hat{D}^{-1}(\xi)\, \mathrm{d}^2\xi$$

onde a função peso

$$\chi(\xi) = \mathbf{Tr}\left[\hat{\rho}\hat{D}(\xi)\right] \tag{6.1.6}$$

é conhecida como *função característica* e seu papel na mecânica quântica estatística é análogo ao da função característica da teoria de probabilidades clássica [13].

6.2 Definição da Função de Wigner

Na teoria de probabilidades clássica, se uma variável aleatória admite uma função densidade de probabilidades, a função característica é sua dual, ou seja, uma é a transformada de Fourier da outra. Com isto em mente partimos da função característica simetricamente ordenada $\chi(\xi)$ e obtemos sua transformada de Fourier complexa:

$$W(\alpha) = \frac{1}{\pi^2} \int \mathrm{d}^2\xi e^{(\alpha\xi^* - \alpha^*\xi)} \chi(\xi) \tag{6.2.1}$$

onde $\alpha = X + iY$.

Esta função tem correspondência com a função introduzida por Wigner, e é o análogo quântico da função de distribuição de probabilidades clássica no plano $X - Y$ (coordenada e momento reescalonados), ou seja, é uma função de distribuição no espaço de fases. Embora seja sempre real e possua muitas das propriedades de uma função de distribuição verdadeira, a função de Wigner pode assumir valores negativos (por exemplo, para os estados de Fock com $n > 0$), dependendo do estado que está sendo representado, razão pela qual é chamada de função de distribuição de *quasi*-probabilidades.

A partir da função de Wigner obtemos as distribuições marginais (e verdadeiras) de probabilidade [15]:

$$P(X) = \int W(X, Y)\, \mathrm{d}Y \tag{6.2.2}$$

$$P(Y) = \int W(X, Y)\, \mathrm{d}X \tag{6.2.3}$$

6.3 Função de Wigner de estados familiares

6.3.1 Função de Wigner do vácuo $|0\rangle$

Calculando o traço com uma expansão sobre os estados coerentes temos a função característica:

$$\begin{aligned}
\chi_v(\xi) &= \mathbf{Tr}\left[|0\rangle\langle 0|\hat{D}(\xi)\right] \\
&= \frac{1}{\pi}\int \langle\alpha|0\rangle\langle 0|\hat{D}(\xi)|\alpha\rangle \,\mathrm{d}^2\alpha \\
&= \frac{1}{\pi}\int e^{-\frac{|\alpha|^2}{2}}\langle 0|\xi+\alpha\rangle\, e^{\frac{1}{2}(\xi\alpha^*-\xi^*\alpha)}\mathrm{d}^2\alpha \\
&= \frac{1}{\pi}\int e^{-\frac{1}{2}\left(|\alpha|^2+|\xi+\alpha|^2+\xi^*\alpha-\xi\alpha^*\right)}\mathrm{d}^2\alpha
\end{aligned}$$

onde utilizamos as expressões [Eq. 4.3.5] e [Eq. 4.3.15]. Inserindo esta expressão no cálculo da função de Wigner obtemos:

$$\begin{aligned}
W_v(\nu) &= \frac{1}{\pi^3}\int\int e^{\nu\xi^*-\nu^*\xi}e^{-\frac{1}{2}\left(|\alpha|^2+|\xi+\alpha|^2+\xi^*\alpha-\xi\alpha^*\right)}\mathrm{d}^2\alpha\mathrm{d}^2\xi \\
&= \frac{1}{\pi^3}\int\int_{-\infty}^{\infty}\int_{-\infty}^{\infty} e^{-\frac{1}{2}\xi_i^2+[-\alpha_i+i(\alpha_r-2\nu_r)]\xi_i-\left[\left(\alpha_i^2+\alpha_r^2+\alpha_r\xi_r+\frac{1}{2}\xi_r^2\right)+i\xi_r(\alpha_i-2\nu_i)\right]}\mathrm{d}\xi_i\mathrm{d}\xi_r\mathrm{d}^2\alpha \\
&= \frac{2}{\pi^2}\int e^{-|\alpha|^2-2|\nu|^2}e^{2\alpha\nu^*}\mathrm{d}^2\alpha \\
&= \frac{2}{\pi}e^{-2|\nu|^2} \qquad (6.3.1)
\end{aligned}$$

Onde chamamos $\alpha=\alpha_r+i\alpha_i$, $\xi=\xi_r+i\xi_i$, $\nu=\nu_r+i\nu_i$, usamos que $\mathrm{d}^2\xi=\mathrm{d}\xi_r\mathrm{d}\xi_i$ e $\mathrm{d}^2\alpha=\mathrm{d}\alpha_r\mathrm{d}\alpha_i$, e aplicamos quatro vezes a fórmula:

$$\int_{-\infty}^{\infty} e^{z_1x^2+z_2x+z_3}\mathrm{d}x=\frac{\sqrt{\pi}}{\sqrt{-a}}e^{-\frac{z_2^2}{4z_1}+z_3} \qquad (6.3.2)$$

onde $\{z_1,z_2,z_3\}\in\mathbb{C}$, $x\in\mathbb{R}$ e $\mathcal{R}(z_1)<0$.

6.3.2 Função de Wigner do estado de Fock $|n=3\rangle$

Fazendo novamente o traço com uma expansão sobre os estados coerentes:

$$\begin{aligned}
\chi_{n=3}(\xi) &= \mathbf{Tr}\left[|3\rangle\langle 3|\,\hat{D}(\xi)\right] \\
&= \frac{1}{\pi}\int \langle\alpha|3\rangle\langle 3|\,\hat{D}(\xi)\,|\alpha\rangle\,\mathrm{d}^2\alpha \\
&= \frac{1}{\pi}\int \left(\frac{\alpha^3}{\sqrt{3!}}e^{-\frac{|\alpha|^2}{2}}\right)^* \left[\frac{(\xi+\alpha)^3}{\sqrt{3!}}e^{-\frac{|\xi+\alpha|^2}{2}}\right] e^{\frac{1}{2}(\xi\alpha^*-\xi^*\alpha)}\mathrm{d}^2\alpha \\
&= \frac{1}{\pi}\int \frac{\alpha^{*3}(\xi+\alpha)^3}{6}e^{-\frac{1}{2}\left(|\alpha|^2+|\xi+\alpha|^2+\xi^*\alpha-\xi\alpha^*\right)}\mathrm{d}^2\alpha
\end{aligned}$$

Inserindo esta expressão no cálculo da função de Wigner obtemos, pelo mesmo procedimento da seção anterior:

$$\begin{aligned}
W_{n=3}(\nu) &= \frac{1}{\pi^3}\int\int e^{\nu\xi^*-\nu^*\xi}\frac{\alpha^{*3}(\xi+\alpha)^3}{6}e^{-\frac{1}{2}\left(|\alpha|^2+|\xi+\alpha|^2+\xi^*\alpha-\xi\alpha^*\right)}\mathrm{d}^2\alpha\mathrm{d}^2\xi \\
&= \frac{2}{\pi}e^{-|\nu|^2}\left[\frac{8}{3}|\nu|^4\left(4|\nu|^2-9\right)+12|\nu|^2-1\right] \qquad (6.3.3)
\end{aligned}$$

6.3.3 Função de Wigner de um estado coerente $|\beta\rangle$

Utilizando o produto escalar entre estados coerentes [Eq. 4.3.18] temos:

$$\begin{aligned}
\chi_{\beta}(\xi) &= \mathbf{Tr}\left[|\beta\rangle\langle\beta|\,\hat{D}(\xi)\right] \\
&= \frac{1}{\pi}\int \langle\alpha|\beta\rangle\langle\beta|\,\hat{D}(\xi)\,|\alpha\rangle\,\mathrm{d}^2\alpha \\
&= \frac{1}{\pi}\int e^{\left(-\frac{1}{2}|\alpha|^2+\alpha^*\beta-\frac{1}{2}|\beta|^2\right)}e^{\left(-\frac{1}{2}|\beta|^2+\beta^*(\xi+\alpha)-\frac{1}{2}|\xi+\alpha|^2\right)}e^{\frac{1}{2}(\xi\alpha^*-\xi^*\alpha)}\mathrm{d}^2\alpha
\end{aligned}$$

Inserindo esta expressão no cálculo da função de Wigner obtemos:

$$\begin{aligned}
W_{\beta}(\nu) &= \frac{1}{\pi^3}\int\int e^{\nu\xi^*-\nu^*\xi}e^{\left(-\frac{1}{2}|\alpha|^2+\alpha^*\beta-\frac{1}{2}|\beta|^2\right)}e^{\left(-\frac{1}{2}|\beta|^2+\beta^*(\xi+\alpha)-\frac{1}{2}|\xi+\alpha|^2\right)}e^{\frac{1}{2}(\xi\alpha^*-\xi^*\alpha)}\mathrm{d}^2\alpha\mathrm{d}^2\xi \\
&= \frac{2}{\pi}e^{-2|\nu-\beta|^2} \qquad (6.3.4)
\end{aligned}$$

Notamos que o deslocamento do estado, no plano das quadraturas, corresponde ao deslocamento de sua distribuição de quasi-probabilidades de Wigner. O mesmo efeito observamos com outras transformações, como a rotação ou a compressão. Isto nos permite obter a função de Wigner de estados mais complicados através de simples transformações, como feito a seguir.

6.3.4 Função de Wigner de um estado comprimido, deslocado e rotacionado $|\alpha, \zeta\rangle = \hat{D}\left(\alpha_0 e^{i\theta}\right)\hat{S}\left(re^{2i\theta}\right)|0\rangle$

Para obtermos a função de Wigner de um estado comprimido com $\zeta = re^{2i\theta}$ e deslocado de $\alpha = \alpha_0 e^{i\theta}$ (a partir do vácuo) torna-se mais fácil aplicarmos estas transformações diretamente sobre a função de Wigner do vácuo, o que equivale a aplicarmos o inverso destas transformações sobre os eixos do espaço de fases.

Iniciamos com a expansão do eixo ν_r e compressão do eixo ν_i por um fator e^r (efeitos inversos na distribuição):

$$\begin{aligned} \nu_r' &= \nu_r e^{-r} \\ \nu_i' &= \nu_i e^{r} \end{aligned}$$

Agora, deslocamos a origem para $(-\alpha_0, 0)$ (o centro da distribuição vai para $(\alpha_0, 0)$):

$$\begin{aligned} \nu_r' &= \nu_r e^{-r} + \alpha_0 = e^{-r}\left(\nu_r + \alpha_0 e^{r}\right) \\ \nu_i' &= \nu_i e^{r} \end{aligned}$$

E a seguir rotacionamos os eixos de um ângulo $-\theta$ (rotacionamos a distribuição de um ângulo θ ao redor da origem):

$$\begin{pmatrix} \nu_r'' \\ \nu_i'' \end{pmatrix} = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} \begin{pmatrix} \nu_r' \\ \nu_i' \end{pmatrix} = \begin{pmatrix} e^{-r}\cos\theta & -e^{r}\sin\theta \\ e^{-r}\sin\theta & e^{r}\cos\theta \end{pmatrix} \begin{pmatrix} \nu_r + \alpha_0 e^{r} \\ \nu_i \end{pmatrix}$$

Finalmente, resolvendo para ν_r e ν_i, encontramos a mudança de variáveis a ser realizada:

$$\nu_r = e^{r}\left(\cos\theta\nu_r'' + \sin\theta\nu_i'' - \alpha_0\right)$$

$$\nu_i = e^{-r}\left(-\sin\theta\nu_r'' + \cos\theta\nu_i''\right)$$

Chamando $\gamma = \nu_r'' + i\nu_i''$ e lembrando que $\alpha_0 \in \mathbb{R}$, podemos escrever estas expressões como:

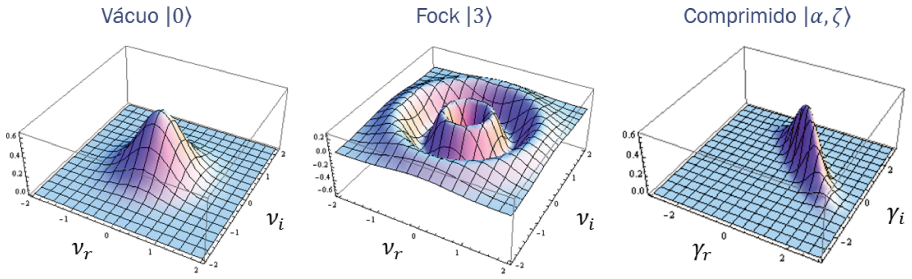


Figura 6.1: Função de distribuição de Wigner dos estados de vácuo $|0\rangle$, de Fock $|3\rangle$ e comprimido $\left|\alpha = 1e^{i\frac{\pi}{4}}, \zeta = 0.7e^{i\frac{\pi}{2}}\right\rangle$.

$$\nu_r = e^r \mathcal{R}\left(\gamma e^{-i\theta} - \alpha_0\right) \tag{6.3.5}$$

$$\nu_i = e^{-r} \mathcal{I}\left(\gamma e^{-i\theta}\right) \tag{6.3.6}$$

Onde as funções $\mathcal{R}$ e $\mathcal{I}$ tomam a parte real e imaginária de seus argumentos, respectivamente. Partindo da [Eq. 6.3.1] e trocando as coordenadas ν_r e ν_i pelas novas coordenadas temos:

$$W_v(\nu) = \frac{2}{\pi} e^{-2\left(\nu_r^2 + \nu_i^2\right)} \Rightarrow W_{\alpha,\zeta}(\gamma)$$

$$W_{\alpha,\zeta}(\gamma) = \frac{2}{\pi} e^{-2\left[e^{2r}\mathcal{R}\left(\gamma e^{-i\theta} - \alpha_0\right)^2 + e^{-2r}\mathcal{I}\left(\gamma e^{-i\theta}\right)^2\right]} \tag{6.3.7}$$

Esta função de Wigner e a função de Wigner do vácuo serão utilizadas nos capítulos 9 e 10 para a descrição dos estados contínuos usados pelos protocolos.

Na Figura 6.1 plotamos a função de Wigner para os estados de vácuo $|0\rangle$, de Fock $|3\rangle$ e comprimido $\left|\alpha = 1e^{i\frac{\pi}{4}}, \zeta = 0.7e^{i\frac{\pi}{2}}\right\rangle$. Da distribuição para o estado de Fock, com $n = 3$, notamos que a função de Wigner nem sempre é positiva.

6.4 A Função de Wigner de dois modos

Para sistemas com duas partículas (modos) podemos generalizar a função característica de forma muito direta [23]:

$$\chi(\mu, \eta) = \mathbf{Tr}\left[\hat{D}(\mu)\hat{D}(\eta)\hat{\rho}\right] \tag{6.4.1}$$

onde $\hat{\rho}$ é o operador densidade do sistema como um todo. Desta forma, definimos a Função de Wigner de Dois Modos:

$$W(\alpha,\beta) = \frac{1}{\pi^4}\int\int \mathrm{d}^2\mu\mathrm{d}^2\eta e^{(\alpha\mu^*-\alpha^*\mu)}e^{(\beta\eta^*-\beta^*\eta)}\chi(\mu,\eta) \tag{6.4.2}$$

Esta definição, nesta forma, será utilizada para a dedução de uma expressão para a relação entre a função de Wigner de entrada e de saída de um divisor de feixes, para dois modos do campo eletromagnético (Apêndice A.3).

Capítulo 7

Os Elementos da Distribuição Quântica de Chaves

Embora *Criptografia Quântica* e *Distribuição Quântica de Chaves* (QKD) sejam termos usados quase indistintamente, a Criptografia Quântica é mais geral, tratando não somente da transmissão de informação, mas também de sua armazenagem e processamento com segurança [33]. Neste texto daremos ênfase à Distribuição Quântica de Chaves, uma solução bastante promissora para o futuro das comunicações secretas.

A busca por uma cifra inquebrável levou ao desenvolvimento do one-time-pad, e esta cifra seria a solução perfeita para o problema das comunicações secretas, não fosse a criação de outro problema quase igualmente complexo: a necessidade de distribuição de chaves completamente secretas (veja a Seção 1.7).

Nas últimas décadas, a distribuição de chaves tem sido feita através de matemática, sendo sua segurança baseada na segurança computacional prática[1] [2, 19]. Entretanto, o problema da distribuição de chaves possui também soluções de caráter físico, como a entrega da chave pessoalmente, e estas soluções são definitivas e incondicionalmente seguras. Dentre estas soluções está a Distribuição Quântica de Chaves, que será apresentada neste capítulo e nos seguintes.

Neste capítulo apresentaremos a estrutura geral dos protocolos de criptografia quântica e os componentes deste tipo de protocolo. A seguir, mostraremos um procedimento de correção de erros e dois procedimentos de ampliação de privacidade. Ao final, discutiremos as leis da física que garantem a segurança das transmissões quânticas.

[1] De fato, hoje a criptografia é considerada um ramo da matemática.

7.1 A Estrutura dos Protocolos de QKD

As leis da natureza (mecânica quântica) não permitem que um determinado estado seja completamente caracterizado em uma única medição. Além disso, determinam que esta medição irá alterar o estado, não sendo possível medir o mesmo estado, com as mesmas características, duas vezes. Esta não é uma limitação tecnológica, mas sim um princípio fundamental da teoria quântica, razão pela qual os protocolos que fazem uso deste princípio são eternamente inquebráveis.

Esta limitação na identificação dos estados transmitidos leva um possível espião a introduzir alterações nestes estados, sendo portanto registradas e reveladas todas as suas ações. Esta é a vantagem do uso da QKD para o *crescimento*[2] de duas sequências aleatórias e idênticas de bits, em dois lugares remotos: a possibilidade de detecção da espionagem ainda durante a transmissão desta chave. Assim, mesmo que o espião conheça a chave completa, ele terá em mãos apenas uma sequência aleatória e nada mais, pois Alice não transmitirá a mensagem tendo detectado a espionagem. Apenas quando Alice e Bob têm certeza de que a transmissão foi bem-sucedida, Alice cifra a mensagem e a envia a Bob pelo canal público. Desta vez, Eva obtém a mensagem cifrada completa mas não conhece a chave, ou seja, novamente possui uma sequência aleatória de bits sem significado [32].

Em geral, nos protocolos de QKD, o procedimento de transmissão da chave envolve três etapas:

Preâmbulos - Alice e Bob utilizam o canal público para definir todos os detalhes dos estados a serem usados, quais serão as bases usadas, como será feita a medição e como será a codificação dos bits (por exemplo: bit 0 - polarização horizontal, bit 1 - vertical, etc).

Transmissão Quântica - Alice produz os bits, gera e transmite os respectivos estados, Eva aplica suas operações de espionagem e Bob faz suas medições.

Comunicação Pública - Alice e Bob voltam ao canal público para que Bob consiga definir quais são seus bits (decodificar os sinais) e Alice possa descartar de seus bits aqueles bits que Bob não possui. Alice e Bob então revelam uma parte de seus bits para que possam obter uma estimativa da taxa de erros e de informações vazadas para Eva.

Ao final da QKD, Bob deve conhecer melhor que Eva os bits de Alice. Caso isso seja verdade, é sempre possível a transmissão de informações com segurança, pois há uma maior quantidade de informações compartilhadas entre Alice e Bob do que entre Alice e Eva. O comprimento

[2] crescimento, pois as partes comunicantes necessitam compartilhar alguma informação prévia, usada para autenticação.

máximo da *chave secreta* é simplesmente $K = I(A,B) - I(A,E)$. Esta chave secreta é obtida através de um processo de purificação da *chave crua*, apresentado nas seções 7.4 e 7.5.

7.2 O Canal Público Autenticado

O canal público pode ser implementado com qualquer tecnologia atual de transmissão de informações, como por exemplo ondas de rádio, fios telefônicos ou pulsos de luz em fibras ópticas. O canal é chamado público pois, sendo regido pela física clássica, qualquer intruso que leia os sinais transmitidos não alterará o sinal recebido, não podendo ser detectado. Assumimos, portanto, que todo e qualquer indivíduo interessado possui acesso integral às transmissões pelo canal público. A autenticação garante que Alice se comunique com Bob sem que as mensagens publicadas sejam alteradas [32].

A grande utilidade do canal público está na sua exatidão. Através dele, Alice e Bob podem se comunicar sem erros ou mal entendidos, podendo, por exemplo, combinar qual será o protocolo usado e todas as suas características. Após a transmissão quantica, Alice e Bob farão a correção de erros na chave e misturarão seus bits de forma a confundir qualquer possível espião, tudo através de discussões pelo canal público. Por fim, Alice irá cifrar sua mensagem com o one-time-pad e irá transmitir o criptograma para Bob através do canal público.

É útil evidenciar aqui a importância da máxima de Shannon, "O inimigo conhece o sistema", para o desenvolvimento de um protocolo, pois o uso constante do canal público revelará a Eva todos os detalhes necessários para que ela seja capaz de realizar o mesmo procedimento de Bob.

7.3 O Canal Quântico

O canal quântico é o meio pelo qual são transmitidos os estados quânticos de Alice para Bob, com ou sem a interferência de Eva. Para fótons, os meios de transmissão mais comuns são as fibras ópticas e o ar. Cada meio tem suas vantagens e desvantagens em termos de absorção, dispersão, introdução de ruídos e alterações na polarização da luz e fase geométrica. Várias dessas características dependem de condições ambientais, como temperatura e umidade, o que requer grande estabilização das condições em que o canal quântico é mantido. Uma vez estabilizadas essas condições, as transmissões tornam-se viáveis através de uma calibração dos parâmetros ajustáveis de Bob e Alice, de forma a compensar quaisquer distorções introduzidas no sinal pelo canal quântico. Para esta calibração, Bob e Alice fazem amplo uso do canal público [32].

A importância do canal quântico reside na sensibilidade dos sinais transmitidos através dele. Regidos pela mecânica quântica, os estados transmitidos registram toda e qualquer tentativa de medição realizada, mudando suas características após cada projeção nos autoestados de um operador observável. Estas cicatrizes são finalmente medidas por Bob e identificadas através de uma comunicação pública com Alice. Ao identificarem a espionagem, Alice e Bob podem partir em busca do espião, consertar o canal quântico e novamente tentar a transmissão sem que o espião tenha tido contato algum com a mensagem, já que apenas uma sequência aleatória de bits (a chave) foi transmitida e vazada.

Alice e Bob podem repetir este procedimento até que a chave tenha sido transmitida com segurança ou podem, por outro lado, guardar esta chave defeituosa e obter uma estimativa da quantidade de informação que foi vazada para Eva. Se esta estimativa for suficientemente pequena, Alice e Bob partem para os procedimentos de correção de erros e ampliação de privacidade, fazendo uso de comunicação pública para encurtar suas chaves e removendo, *se fosse possível*[3], apenas os bits errados e os bits conhecidos por Eva.

7.4 A Correção de Erros

Após a transmissão dos sinais quânticos, Alice e Bob possuem dados clássicos altamente vinculados, porém não idênticos. Os ruídos e perdas (e/ou possível espionagem), e mesmo a pequena sobreposição natural entre os estados (principalmente para os protocolos de variáveis contínuas), introduzem erros nos bits medidos por Bob. Para que as chaves sob o poder de Alice e Bob sejam praticamente idênticas é necessário um pós processamento capaz de remover os bits errados[4].

Aqui apresentamos um algoritmo simples de correção de erros, proposto por Bennett em 1992 [19]. Este procedimento é válido para qualquer par de chaves compartilhadas que possuam alguns bits diferentes entre si. Os protocolos de QKD geram estas chaves compartilhadas e também uma estimativa de erros. Na Figura 7.1 todo o procedimento é explicitado através de um exemplo. Nota-se que grande parte dos bits é descartada na busca pelos bits errados.

[3]Sempre há uma grande "queima" de bits durante a correção de erros e ampliação de privacidade. Esse desperdício se deve ao fato de Alice e Bob fazerem uma "busca cega" pelos bits errados, já que um não conhece os bits do outro, e também fazerem uso do canal público para comunicação, revelando cada vez mais bits de suas chaves a cada etapa.

[4]A correção de erros não é restrita à criptografia quântica e é, na realidade, muito mais antiga. Algoritmos de correção de erros são largamente implementados nos sistemas computacionais atuais, garantindo a integridade dos dados transmitidos e armazenados.

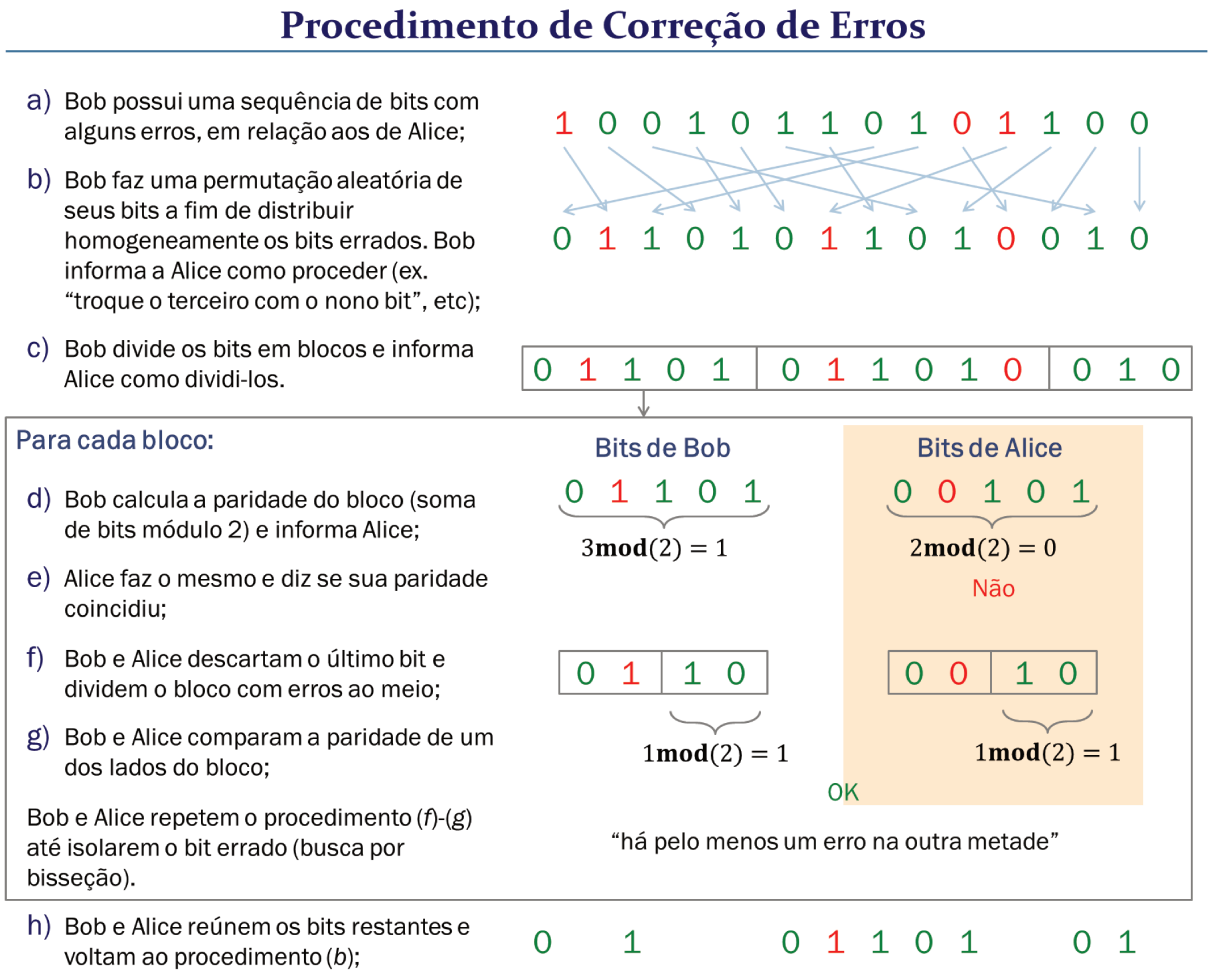


Figura 7.1: Procedimento de correção de erros proposto por Bennett em 1992. (a) Bob e Alice possuem também uma estimativa da taxa de erros. (b) Em nenhum momento Bob ou Alice divulgam seus bits. (c) Usando a taxa de erros, Bob estima que a chave contém n bits errados. Bob divide então os bits em n blocos de tamanho aleatório, de forma que cada bloco contenha apenas um erro em média. (d) e (e) É necessário notar que um número par de erros em um bloco leva a uma mesma paridade, mascarando o bit errado. Isto implica na necessidade de se refazer o procedimento completo algumas vezes. (f) Divulgar a paridade corresponde a divulgar um bit de informação e isto é compensado pelo descarte de um bit. (g) Alice e Bob iniciam uma *busca por bisseção*. (h) Quando a busca tornar-se ineficiente, Bob e Alice comparam a paridade de conjuntos aleatórios de bits, comprovando sua semelhança (para cada comparação, um bit é descartado).

7.5 A Ampliação de Privacidade

Neste ponto, Alice e Bob possuem chaves praticamente idênticas, mas Eva possui conhecimento sobre parte desta chave. Alice e Bob precisam então combinar uma operação sobre os bits, de forma a misturá-los e reduzi-los a uma porção menor, forçando Eva a imitar o mesmo procedimento. Eva, sem escolhas, combina seus bits corretos com os bits errados, de forma arquitetada para que o número de bits seja reduzido, mas o número de erros não. A repetição deste processo faz com que a informação que Eva possui da chave encurtada tenda assintoticamente a zero. A quantidade a ser encurtada na chave é previamente calculada a partir de uma estimativa da quantidade de informações vazadas para Eva, fornecida pelo protocolo de QKD. A seguir, apresentamos dois exemplos de procedimentos de ampliação de privacidade [32].

7.5.1 Pelo uso de uma operação XOR

Alice e Bob realizam uma *operação XOR* (soma de bits módulo 2) em sequências aleatórias de bits, retirados da chave. A escolha destes bits é feita por Bob (ou Alice) e informada a Alice (ou Bob) através do canal público. O comprimento destas sequências é escolhido de forma a encurtar a chave crua apenas na quantidade necessária para que Eva possua uma informação praticamente nula da chave (conforme a estimativa de informações vazadas fornecida pelo protocolo de QKD). Na Figura 7.2, está representada toda a operação de ampliação de privacidade, por operação XOR, para uma pequena sequência de bits.

Se Eva conhece os valores de cada bit apenas com probabilidade $p = \frac{1}{2}(1+\epsilon)$, ela saberá a paridade de cada conjunto de N bits com probabilidade:

$$p' = \frac{1}{2}\left(1+\epsilon^N\right) \tag{7.5.1}$$

Desta forma, quando a sequência de bits é muito longa e a chave é encurtada na medida certa, os bits de Eva estão muito próximos de estarem apenas 50% corretos (como qualquer sequência aleatória) [32].

7.5.2 Pelo uso de uma função HASH

Devido às características das funções Hash (veja a Seção 2.4.3), que reduzem e misturam uma sequência de bits de maneira muito complexa, elas podem ser usadas para ampliação de privacidade [1].

Para isto, Alice e Bob aplicam uma função Hash sobre a chave crua e utilizam o resultado como chave secreta:

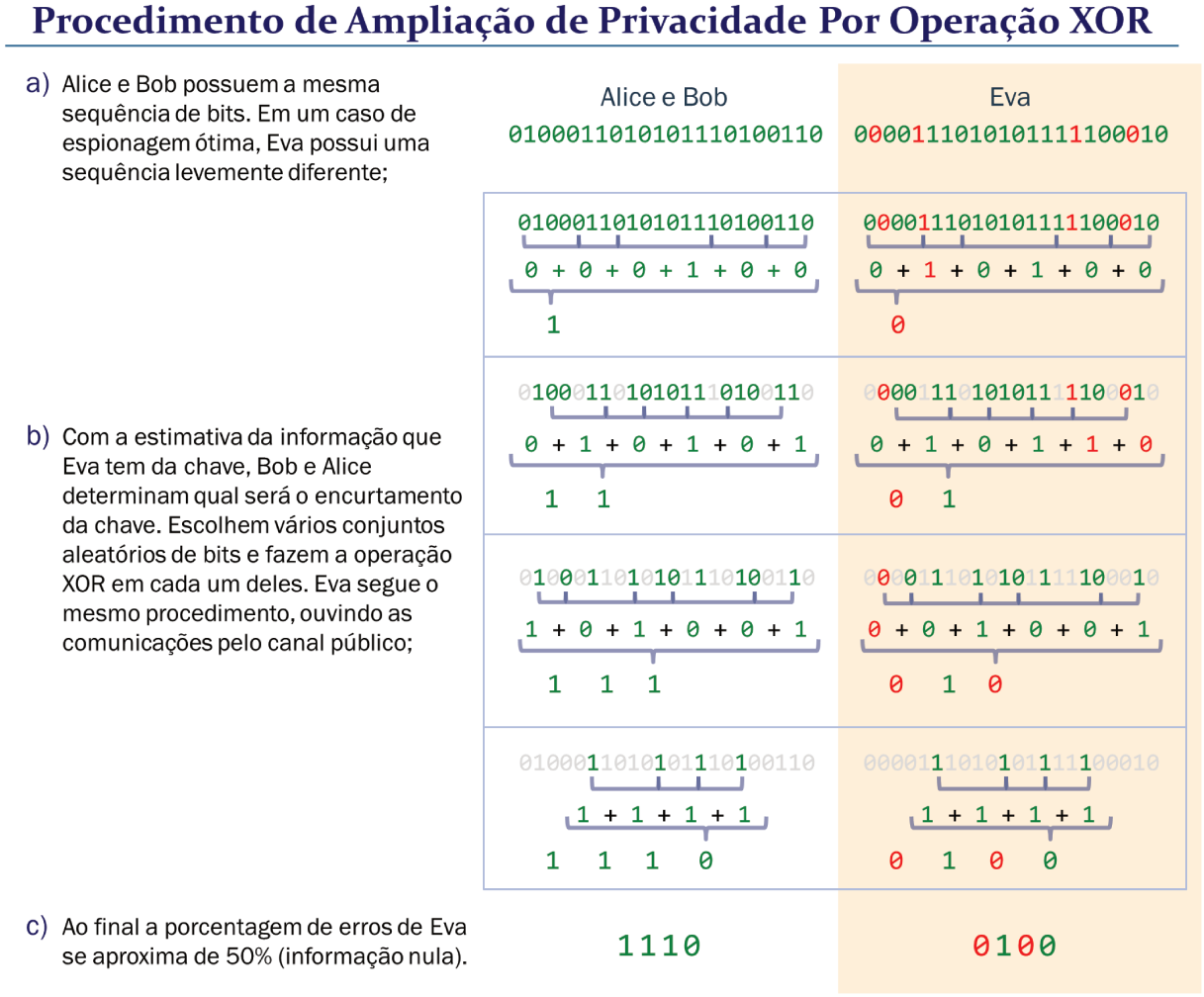


Figura 7.2: Procedimento de Ampliação de Privacidade através do uso da operação XOR. (a) Uma chave secreta pode, a princípio, ser gerada a partir de qualquer chave crua desde que Bob possua mais informações sobre a chave do que Eva. (b) Note que não necessariamente os bits de Eva resultantes estarão errados. Isto é importante pois se Eva obtivesse todos os bits errados, ao final ela poderia simplesmente inverter seus valores, encontrando a chave secreta. (c) As probabilidades de combinação dos bits corretos com bits errados geram uma sequência de bits aleatórios em relação à chave secreta. É esta aleatoriedade que se traduz em informação nula, conforme apresentado na Seção 3.6.

$$h_n(01000110101011101001 10) = 010101010011$$

Eva tenta o mesmo procedimento e obtém:

$$h_n(01001110100011101000 10) = 100111000101$$

Novamente os bits de Eva tendem assintoticamente a estarem apenas 50% corretos.

Para a aplicação deste tipo de função, os bits e Alice e Bob devem estar perfeitamente idênticos, pois quaisquer diferenças podem levar a duas sequências de bits quase completamente não correlacionadas.

7.6 O Teorema da "Não-Clonagem"

Nesta seção demostraremos que a Mecânica Quântica impede a clonagem perfeita de um estado desconhecido. Esta é a lei fundamental de segurança de qualquer protocolo de QKD, já que impede que um espião faça uma cópia de cada estado transmitido e possa posteriormente realizar medições completas em suas cópias sem ser detectado [34, 32].

Suponha que exista uma transformação unitária capaz de realizar uma cópia perfeita de um determinado estado. Esta transformação lê o estado e altera um outro estado preparado convenientemente (chamado $|branco\rangle$), deixando-o idêntico ao estado lido. Suponha que esta cópia possa ser feita para dois estados:

$$\begin{aligned} |branco\rangle\,|a\rangle &\overset{U}{\rightarrow} |a\rangle\,|a\rangle \\ |branco\rangle\,|b\rangle &\overset{U}{\rightarrow} |b\rangle\,|b\rangle \end{aligned} \tag{7.6.1}$$

Queremos agora realizar a cópia de um estado que seja uma combinação linear destes estados:

$$|branco\rangle\,(\alpha\,|a\rangle + \beta\,|b\rangle) = \alpha\,|branco\rangle\,|a\rangle + \beta\,|branco\rangle\,|b\rangle \overset{U}{\rightarrow} \alpha\,|a\rangle\,|a\rangle + \beta\,|b\rangle\,|b\rangle \tag{7.6.2}$$

Nesta transformação, notamos que os estados de saída não estão na forma de um produto direto, como seria o caso de dois estados idênticos e separados:

$$(\alpha\,|a\rangle + \beta\,|b\rangle)\,(\alpha\,|a\rangle + \beta\,|b\rangle) = \alpha^2\,|a\rangle\,|a\rangle + \alpha\beta\,|a\rangle\,|b\rangle + \beta\alpha\,|b\rangle\,|a\rangle + \beta^2\,|b\rangle\,|b\rangle \tag{7.6.3}$$

A cópia, portanto, está incorreta. Tendo suposto a possibilidade de cópia dos estados $|a\rangle$

e $|b\rangle$, podemos supor a possibilidade de cópia de um estado $|c\rangle = (\alpha\,|a\rangle + \beta\,|b\rangle)$. Entretanto, esta cópia terá de ser feita por uma nova transformação unitária que, por sua vez, não será capaz de copiar $|a\rangle$ ou $|b\rangle$. Esta necessidade de uma transformação de cópia para cada estado recebido implica na necessidade de conhecimento de qual estado está sendo recebido. Se o espião não conhece de antemão o estado recebido, a cópia não será sempre perfeita. Este é o fundamento do *teorema da não-clonagem de estados desconhecidos*.

7.7 O Teorema da "Não-Sondagem"

Veremos adiante que alguns protocolos fazem uso de apenas *2 estados quânticos não ortogonais*. Nesta seção será demonstrada a segurança de tais protocolos [32, 34].

Suponha que exista uma transformação unitária capaz de ao menos alterar o estado de uma sonda através de sua interação com o estado transmitido, capturando alguma informação dos estados sem alterá-los:

$$\begin{aligned} |E\rangle\,|a\rangle &\overset{\mathrm{U}}{\rightarrow} |E_a\rangle\,|a\rangle \\ |E\rangle\,|b\rangle &\overset{\mathrm{U}}{\rightarrow} |E_b\rangle\,|b\rangle \end{aligned} \tag{7.7.1}$$

A unitariedade da evolução quântica exige que o produto interno seja conservado:

$$\langle E|\,\langle a|\,\mathrm{U}^{\dagger}\mathrm{U}\,|b\rangle\,|E\rangle = \langle a|b\rangle\,\langle E|E\rangle \;\;=\;\; \langle E_a|\,\langle a|b\rangle\,|E_b\rangle = \langle a|b\rangle\,\langle E_a|E_b\rangle \tag{7.7.2}$$

Se os estados forem não-ortogonais, $\langle a|b\rangle \neq 0$, e temos que

$$\langle E_a|E_b\rangle = 1 \tag{7.7.3}$$

Ou seja, a interação de uma sonda com um estado (mediada por uma transformação unitária) não permite a extração de informações sem que o estado seja alterado, pois a sonda é deixada em um mesmo estado final.

Parte III

Criptografia Quântica: Um novo Paradigma

Capítulo 8

A Infância da Criptografia Quântica

Neste capítulo apresentaremos, com uma breve abordagem histórica, o primeiro protocolo de QKD proposto (BB84) e sua versão simplificada para dois estados (B92). Estes protocolos são chamados de *protocolos de variáveis discretas*, pois a decodificação dos bits é feita através da medição de uma variável que pode resultar em apenas alguns valores discretos, como "polarização vertical" ou "polarização horizontal", por exemplo [3, 32].

Apenas após a primeira realização prática de uma QKD a atenção da comunidade científica se voltou para a criptografia quântica. Desde então esta área tem se desenvolvido rapidamente. Novos conceitos de protocolos têm surgido todos os anos e dentre eles temos protocolos que fazem uso de estados discretos emaranhados (E91, BBM92), estados contínuos emaranhados (SKL02) ou não (GG02 , NH03, H04) e com codificação contínua (GG02) ou discreta (NH03, H04) [37, 38, 39].

Ao final deste capítulo serão apresentados alguns ataques mais comuns aos sistemas criptográficos clássicos e quânticos.

8.1 Stephen Wiesner e o Dinheiro Quântico

Por volta de 1970, Stephen Wiesner escreveu um *paper* intitulado "*Conjugate Coding*". Neste trabalho, Wiesner introduziu o conceito de codificação em observáveis quânticos conjugados, mostrou como duas mensagens poderiam ser enviadas de forma que apenas uma pudesse ser lida, mostrou como armazenar e transmitir informações e ilustrou esta idéia com o design de notas de dinheiro impossíveis de serem falsificadas (veja a Figura 8.1). Muitas das idéias de Wiesner permanecem ainda impraticáveis[1], mas representam o primeiro uso da mecânica

[1]Mesmo com toda a tecnologia hoje existente, uma nota de dinheiro quântico teria o tamanho de um carro, custaria muito mais que um carro para ser fabricada e duraria apenas alguns segundos. Devido ao pioneirismo de Wiesner, este trabalho foi rejeitado por quatro revistas diferentes, sendo publicado apenas em

quântica de maneira similar à que é feita hoje em dia na Criptografia Quântica [34].

8.2 Protocolo BB84

Wiesner, frustrado com o pouco acolhimento de suas idéias, decidiu procurar Charles H. Bennett, conhecido por ter uma "mente aberta". Bennett imediatamente reconheceu a relevância do trabalho de Wiesner e mais tarde encontraria Gilles Brassard[2], com quem buscaria uma solução para o problema da distribuição de chaves utilizando a mecânica quântica.

Conta-se que em 1984, após uma longa consideração sobre o problema da distribuição de chaves, Bennett e Brassard tiveram um momento de *eureka* [2] e encontraram uma solução. Partindo da percepção de que "Deus não criou os fótons como um meio de armazenagem, mas sim como um meio de comunicação" [33], Bennett e Brassard puderam adaptar a idéia do dinheiro quântico e formular o primeiro protocolo de criptografia quântica: o Bennett-Brassard-84.

O *paper* original de Bennett e Brassard é tido como o fundador da Criptografia Quântica. Sua simplicidade, precisão e brevidade fazem com que seja considerado, ainda, a melhor introdução a esta área. As implementações mais bem sucedidas para a distribuição quântica de chaves fazem uso do BB84, existindo, inclusive, *kits* comerciais oferecidos por empresas especializadas em segurança [34, 18].

8.2.1 Funcionamento do Protocolo

Para a transmissão dos bits que compõem a chave, o protocolo BB84 utiliza um fóton por bit. A codificação é feita pela polarização do fóton em uma de quatro direções distintas, previamente combinadas com o destinatário (Bob). Estas polarizações são lineares, todas contidas no plano perpendicular à direção de propagação, e são divididas em duas bases, retangular (R) e diagonal (D). Na base retangular estão os fótons com polarização horizontal ($\theta = 0$) ou vertical ($\theta = \pi/2$), codificando respectivamente os bits 0 ou 1. Na base diagonal estão os fótons com polarização na diagonal principal ($\theta = \pi/4$) ou secundária ($\theta = 3\pi/4$), codificando também os bits 0 ou 1, respectivamente. Para cálculos, representamos os quatro estados utilizados através de kets. A Figura 8.2 apresenta, de forma organizada, os quatro estados utilizados. Devido à escolha, os quatro estados enviados não são todos ortogonais

1983 na revista ACM SIGACT News [29]. Ao apresentar suas idéias para amigos e professores, estes logo as ignoravam [34].

[2]Brassard, em uma de suas palestras gravadas em vídeo (veja "Sites, Multimídias e Outros" ao final deste texto), conta como foi o encontro com Bennett. Em uma praia, Bennett o teria abordado dizendo "eu sei como fazer um protocolo de criptografia inquebrável". Esta e outras histórias foram publicadas sob seu ponto de vista [33].

entre si, havendo sempre sobreposição entre os estados de uma base e os estados de outra. É esta sobreposição que implica na introdução de erros por uma espionagem [30, 34].

Após combinarem estas definições pelo *canal público*, Alice e Bob dão início à transmissão. Na Figura 8.3 estão todos os passos do protocolo com a representação de uma transmissão. A *discussão pública* ocorre também pelo canal público, um canal clássico em que tudo o que é transmitido pode ser interceptado por terceiras pessoas, sem alterações no sinal. A única restrição é que o remetente seja autenticado.

Todos os bits e sorteios devem ser verdadeiramente aleatórios, como discutido ao fim da Seção 1.6, ou o espião pode encontrar vínculos entre os bits transmitidos.

8.2.2 Primeira realização prática

A inexistência de fontes de um fóton à época da proposição do protocolo pesou sobre sua credibilidade e difusão, e novamente a criptografia quântica palpitava em silêncio. Apenas no verão de 1989, no Centro de Pesquisas Thomas J. Watson da IBM, Charles H. Bennett e John A. Smolin, conduziram a primeira transmissão quântica de chaves da história. Como fonte de um fóton utilizaram um diodo emissor de luz, que emitia pulsos atenuados através de uma lente e um orifício estreito. Quase todas as peças da montagem foram obtidas do depósito da IBM e muitos improvisos foram feitos [35, 18, 2].

8.3 Protocolo B92

Em 1992, Bennett, após trabalhar no desenvolvimento do protocolo BBM92, notou que a segurança do protocolo BB84 (ou qualquer outro protocolo que não faça uso de emaranhamento) está baseada no fato de que a realização de qualquer medida que não altere o estado transmitido não pode extrair informação alguma desse estado (veja a Seção 7.7). Este fato permitiria então o desenvolvimento de um protocolo que fizesse uso de apenas dois estados não-ortogonais [36].

8.3.1 Funcionamento do Protocolo

Para a identificação de dois estados $|A\rangle$ e $|B\rangle$, com $\langle A|B\rangle \neq 0$, pode-se usar como medida dois projetores nos espaços ortogonais a cada estado: $P_A = I - |B\rangle\langle B|$ e $P_B = I - |A\rangle\langle A|$. Desta forma, medir com o projetor correto (por exemplo, P_A sobre $|A\rangle$) tem uma probabilidade não nula de dar um resultado, enquanto medir com o projetor errado (por exemplo, P_A sobre $|B\rangle$) sempre dará um resultado nulo [34].

Em uma implementação com polarização de fótons, Alice e Bob combinam quais os dois estados que serão usados. Digamos que escolham os estados de polarização horizontal ($\theta = 0$, estado $|A\rangle$), representando o bit 0, e polarização na diagonal secundária ($\theta = \pi/4$, estado $|B\rangle$), representando o bit 1. Os projetores que Bob usaria poderiam ser implementados na forma de um simples polarizador, rotacionado de forma a bloquear completamente luz polarizada com $\theta = \pi/4$ (projetor P_A), ou de forma a bloquear luz com $\theta = 0$ (projetor P_B). Os passos do protocolo e uma transmissão de exemplo estão representados na Figura 8.4.

Embora seja ainda bastante difícil de ser implementado, o protocolo B92 demonstrou a possibilidade de transmissão segura de chaves através de apenas dois estados com projeção não nula um sobre o outro (não-ortogonais). A codificação pode ser realizada através de polarizações, amplitudes, fases, etc. Em particular, os protocolos de variáveis contínuas dos capítulos seguintes se aproveitarão de estados da luz cujas amplitudes ou fases apresentam sobreposição.

8.4 Ataques e Soluções

Nesta seção apresentaremos alguns ataques fundamentais tanto da criptografia clássica quanto da criptografia quântica [32]. Naturalmente, existe uma infinidade de ataques possíveis, delineados pela mente criativa do espião, o que dificulta grandemente a análise de segurança de um protocolo. Em geral procura-se um ataque que, acredita-se, seja o melhor ataque possível ao protocolo proposto, e a partir dele são calculados alguns valores limitantes para o protocolo, bem como uma estimativa para a taxa de bits vazados para Eva. Nos capítulos seguintes serão analisados dois ataques para protocolos de variáveis contínuas, um do tipo intercepta-reenvia e outro semelhante ao ataque do divisor de feixes.

8.4.1 Ataque do Homem-no-Meio (*Man-in-the-Middle Attack*)

Neste ataque, Eva se comunica com Alice fingindo ser Bob e se comunica com Bob fingindo ser Alice. A mecânica quântica não provê meios especiais para que os verdadeiros emissores e receptores possam se identificar com certeza, razão pela qual mesmo a criptografia quântica não é imune a este ataque.

A solução para este ataque é clássica: Alice e Bob precisam compartilhar uma pequena chave inicial. Esta chave é usada para a autenticação (veja a Seção 2.4.4) das partes comunicantes, garantindo que Alice se comunique realmente com Bob e Eva apenas possa ouvir a conversa pública.

8.4.2 Ataque Intercepta-Reenvia (*Intercept-Resend Attack*)

Neste tipo de ataque, Eva recolhe e mede todo o sinal quântico durante toda a transmissão ou durante apenas alguns dos pulsos. Eva tem como tarefa identificar o estado enviado por Alice a fim de reconhecer o bit da chave e de reproduzi-lo a Bob, para que este também possa medi-lo.

Para o BB84, Eva deve escolher dentre duas bases para medição. Quando Eva acerta a base, identifica corretamente o estado com 100% de chances, não modificando o estado a ser recebido por Bob. Já quando erra, suas chances caem para 50%, e metade das vezes Eva envia um estado diferente do que seria esperado por Bob, introduzindo erros nos bits não descartados por Bob. Se Eva intercepta n pulsos de Alice, a probabilidade de Alice e Bob encontrarem erros nos respectivos bits é de $P(n) = 1 - (3/4)^n$, que para a curta sequência de 30 bits já resulta $P(30) \approx 0,999821$ [32].

Se a informação compartilhada entre Alice e Bob I_{AB} for maior que aquela compartilhada entre Alice e Eva I_{AE}, a solução para este ataque é a ampliação de privacidade, caso contrário, torna-se impossível o crescimento de uma chave segura. Para o BB84, devido à possibilidade deste tipo de ataque, uma taxa de erros no canal superior a 25% impede a QKD.

8.4.3 Ataque de Número de Fótons / Divisor de Feixes (*Photon Number / Beam Splitting Attack*)

Estes ataques se aproveitam do não amadurecimento tecnológico de partes comunicantes que fazem uso de protocolos implementados com pulsos de *um fóton*. Atualmente não existem fontes perfeitas de um fóton. Os melhores esquemas de geração produzem pares e trios de fótons com baixas probabilidades. Eva realiza uma medição não destrutiva do número de fótons nos pulsos e, para os pulsos com mais de um fóton, Eva recolhe um dos fótons e o armazena em uma memória quântica, aguardando até a divulgação das bases corretas de medição. Alice e Bob utilizam o outro fóton e acabam compartilhando alguns de seus bits com Eva.

A detecção destes ataques é feita com o uso de pulsos isca (*decoy states*) [32], pulsos mais fortes com grande probabilidade de conterem dois ou mesmo três fótons ou mais. Eva não sabe se o pulso é uma isca ou não e se vê obrigada a dividi-lo, removendo fótons. Alice então diz a Bob quais pulsos deveriam ser mais fortes e Bob identifica a espionagem, obtendo uma estimativa para o número de bits conhecidos por Eva.

A QKD é ainda possível nestes ataques mas a ampliação de privacidade é severa e consome muitos bits da chave crua.

8.4.4 Ataque de Burla (*Hacking Attack*)

Nesta classe de ataques, Eva tira qualquer proveito possível de toda espécie de falha na implementação do protocolo. Como exemplo, um gerador de fótons, cuja saída possua uma superfície bastante reflexiva, pode ser usado para refletir um pulso forte de Eva através do polarizador de Alice, de volta pelo polarizador até Eva. Desta forma, Eva conhecerá todas as polarizações dos estados sem interferir com sua transmissão.

8.4.5 Ataque por Negação de Serviço (*Denial Of Service Attack*)

Neste ataque, Eva bloqueia completamente os sinais, forçando Alice e Bob a mudarem de estratégia de transmissão.

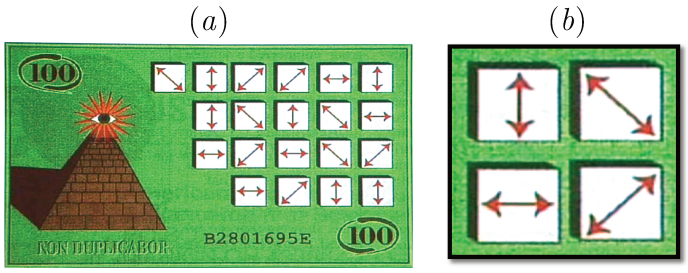


Figura 8.1: (*a*) *Unforgeable Bank Notes.* A nota de dinheiro quântico conteria diversas caixinhas com estados quânticos guardados, preparados em duas bases ortogonais, conhecidos apenas pelo banco. Qualquer medição em base errada realizada por um falsificador estragaria a nota, pois projetaria o estado em outro. O banco, ao receber a nota, faria uso de seu número de série para saber quais bases usar nas medições, sendo capaz de detectar uma tentativa de falsificação com grande probabilidade. (*b*) Detalhe dos 4 estados distintos. (Imagem retirada da apresentação em vídeo de Brassard A.3).

Base	Bit	Estado	Representação
R	0	$\|0\rangle_R$	↔
	1	$\|1\rangle_R$	↕
D	0	$\|0\rangle_D = \frac{1}{\sqrt{2}}(\|0\rangle_R + \|1\rangle_R)$	↗
	1	$\|1\rangle_D = \frac{1}{\sqrt{2}}(\|0\rangle_R - \|1\rangle_R)$	↘

Figura 8.2: Polarização dos fótons em base retangular e diagonal. Os fótons da base diagonal podem ser descritos em termos dos fótons da base retangular e vice-versa.

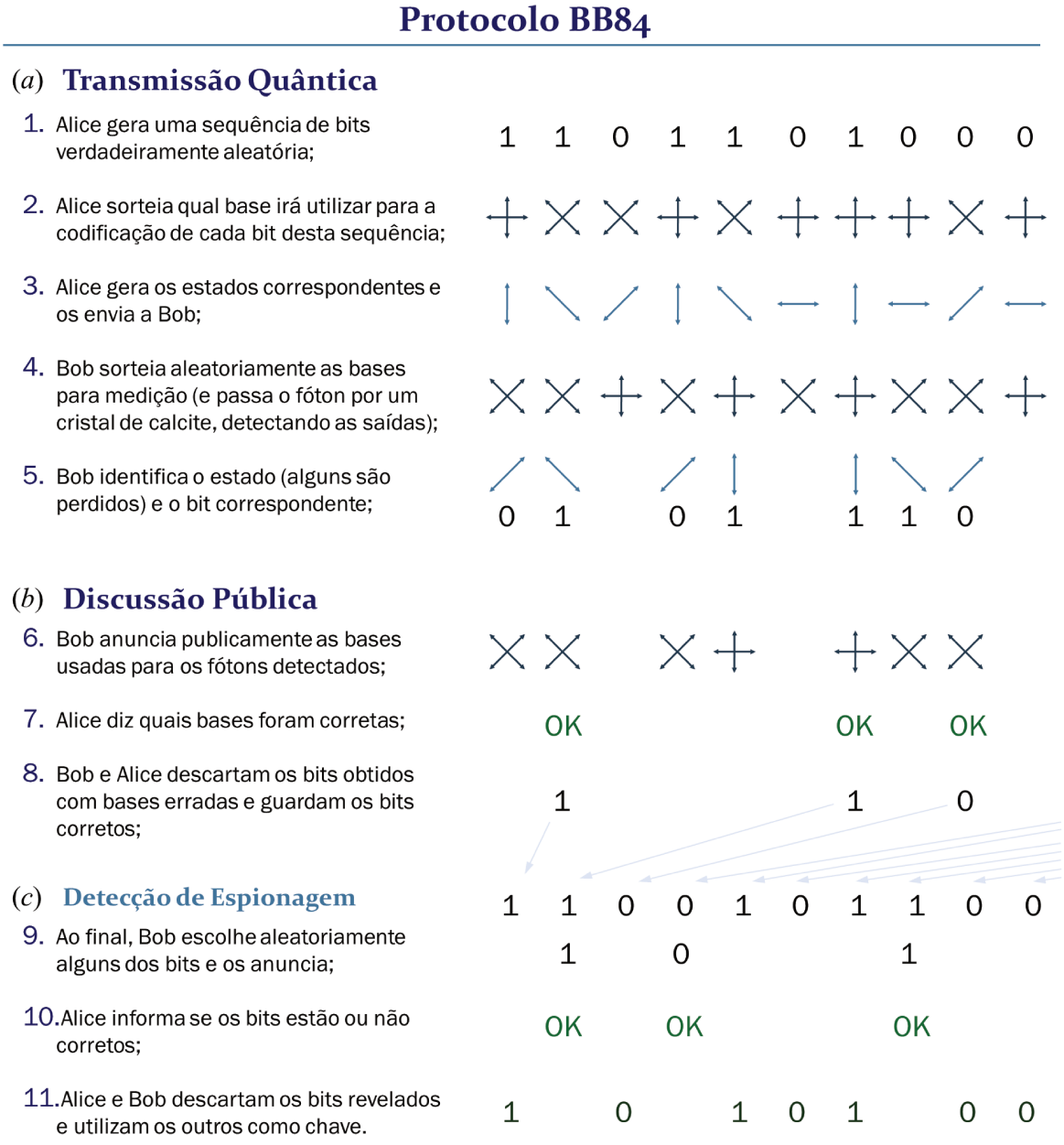


Figura 8.3: Exemplo de transmissão do Protocolo BB84. (a) Durante a transmissão quântica ocorre perda de alguns fótons. (b) Na discussão pública são selecionados os bits que deveriam estar corretos. (c) Usando ainda o canal público é feita uma estimativa da taxa de erros nos bits aceitos através da comparação de uma fração dos bits de Alice e Bob. Qualquer erro deve ser atribuído à existência de um espião (cenário paranóico). Neste exemplo não há espionagem, implicando em uma taxa de erros nula. Em uma situação real, para qualquer taxa de erros diferente de zero, a segurança e correteza da chave só pode ser garantida após a correção de erros e ampliação de privacidade (veja a Seção 7.4).

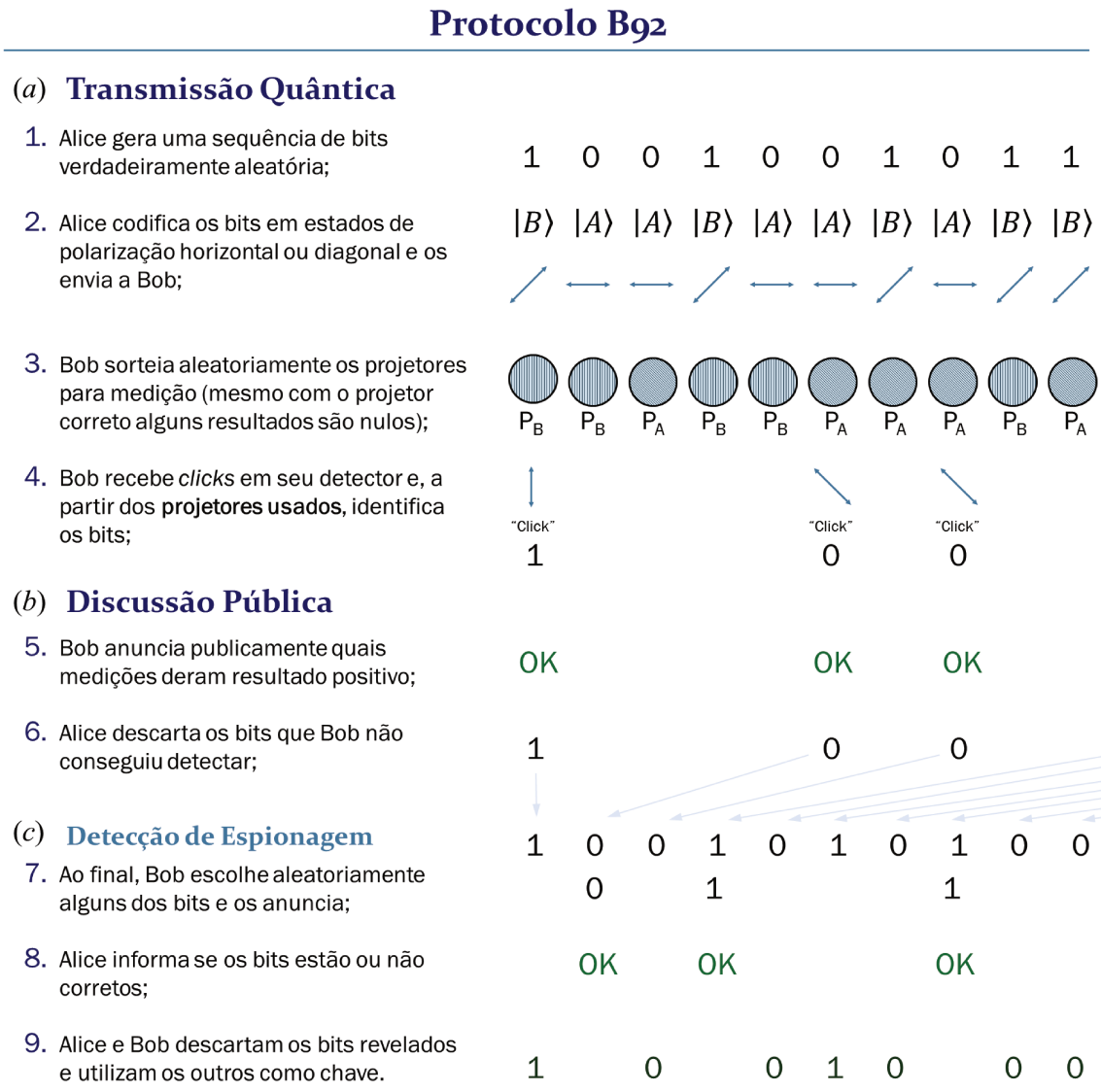


Figura 8.4: Exemplo de transmissão com o protocolo B92. (a) Ao final da transmissão quântica, Bob conhece alguns bits de Alice, mas Alice não sabe quais. (b) Alice é informada sobre quais de seus bits foram identificados por Bob. (c) Na ausência de um espião os bits comparados devem coincidir perfeitamente. Caso contrário, a partir da porcentagem de bits errados, Alice e Bob podem calcular quanta informação Eva tem da chave e o quanto a chave crua deve ser reduzida para se tornar secreta.

Capítulo 9

Criptografia Quântica com Variáveis Contínuas

A partir deste ponto abordaremos os *protocolos com variáveis contínuas*, cuja implementação é mais vantajosa do ponto de vista tecnológico, devido às maiores facilidades de produção, transmissão e detecção dos estados usados.

9.1 Protocolo NH03

Nesta seção introduziremos o conceito de protocolo com variáveis contínuas através de um exemplo simples de protocolo com codificação discreta, proposto por Namiki e Hirano em 2003 [38].

Namiki e Hirano observaram que a medição de quadratura por detecção homódina balanceada envolve uma operação de deslocamento de fase (*phase-shift*) e que as fontes mais convencionais são fontes de pulsos de luz coerente. Sendo assim, uma combinação de moduladores de fase e detecção homódina deveria fornecer um esquema simples, do ponto de vista experimental, para protocolos de QKD com variáveis contínuas. Com isto em mente, apresentaram um protocolo em que a codificação dos bits seria feita em 4 estados coerentes de amplitude $\alpha > 0$, com deslocamentos de fase de $\pi/2$ entre si, e a decodificação seria feita pela medida de uma das duas quadraturas $\left\{\hat{X}, \hat{Y}\right\}$ do campo, onde $\hat{a} = \hat{X} + i\hat{Y}$. O funcionamento deste protocolo é análogo ao BB84:

9.1.1 Funcionamento do Protocolo

Para cada pulso, Alice escolhe aleatoriamente um dentre os quatro estados coerentes $\{|\alpha\rangle, |i\alpha\rangle, |-\alpha\rangle, |-i\alpha\rangle\}$ e o envia a Bob;

A seguir, Bob escolhe aleatoriamente uma das duas quadraturas ($\hat{X}$ ou $\hat{Y}$) e mede o pulso recebido;

Alice e Bob se comunicam pelo canal público e dividem seus dados em dois grupos: *bases corretas*, se Alice enviou $|\pm\alpha\rangle$ e Bob mediu $\hat{X}$ ou Alice enviou $|\pm i\alpha\rangle$ e Bob mediu $\hat{Y}$; e *bases erradas*, nos outros casos possíveis;

Para cada pulso medido na base correta, Bob possui um valor x para a quadratura e decodifica o bit correspondente através da regra:

$$(\text{valor do bit}) = \begin{cases} 1 & \text{se } x > x_0 \\ 0 & \text{se } x < -x_0 \\ \textit{inconclusivo} & \text{em outros casos} \end{cases}$$

Os resultados inconclusivos são comunicados a Alice para que ambos possam descartá-los. Este procedimento é chamado de pós-seleção e o valor $x_0 \geqslant 0$ é chamado de limiar de pós-seleção. Seu papel é reduzir a taxa de erros nos bits de Alice e Bob, devido à sobreposição entre os estados ao redor da origem. Outra função é a de reduzir as informações de Eva sobre a chave, permitindo a transmissão por distâncias maiores. O efeito desse limiar sobre as distribuições recebidas por Eva no caso de ataque por troca do canal por canal superior será analisado mais detalhadamente na Seção 10.5.

Por fim, Alice cria sua sequência de bits atribuindo bit 1 aos estados $\{|\alpha\rangle, |i\alpha\rangle\}$ e bit 0 aos estados $\{|-\alpha\rangle, |-i\alpha\rangle\}$ enviados e detectados com base correta.

9.1.2 Detecção da Espionagem

Mesmo conhecendo a forma dos quatro tipos de estados a serem enviados, um espião não pode identificar com certeza um estado particular transmitido devido à sua não-ortogonalidade com os outros estados. Ao errar nesta identificação, necessariamente o espião modifica o estado transmitido e introduz erros nos dados de Bob. Aqui, apenas explicitaremos o efeito dessa espionagem sobre a distribuição recebida por Bob, deixando uma análise mais cuidadosa para a seção seguinte, o protocolo de Horak, que é uma generalização deste protocolo para estados comprimidos da luz.

Devido à aleatoriedade nas escolhas de Alice, os quatro estados aparecem com igual probabilidade durante a transmissão e este conjunto de estados pode ser representado pelo operador densidade:

$$\hat{\rho} = \frac{1}{4}\left(|\alpha\rangle\langle\alpha| + |-\alpha\rangle\langle-\alpha| + |i\alpha\rangle\langle i\alpha| + |-i\alpha\rangle\langle-i\alpha|\right) \tag{9.1.1}$$

Quando Alice anuncia qual foi a base utilizada (qual quadratura foi usada para a codifi-

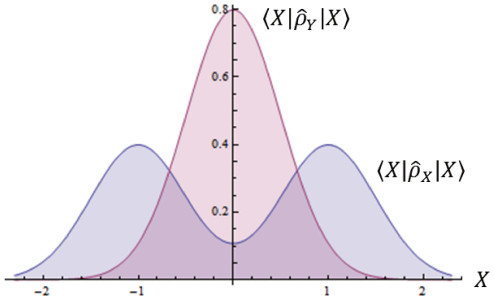


Figura 9.1: (Azul) Distribuição esperada por Bob na ausência de espionagem e (Vermelho) Distribuição recebida por Bob caso Eva intercepte e erre todos os estados.

cação do bit, $\hat{X}$ ou $\hat{Y}$) o operador densidade se reduz a dois casos possíveis:

$$\hat{\rho}_X = \frac{1}{2}\left(|\alpha\rangle\langle\alpha| + |-\alpha\rangle\langle-\alpha|\right) \tag{9.1.2}$$

$$\hat{\rho}_Y = \frac{1}{2}\left(|i\alpha\rangle\langle i\alpha| + |-i\alpha\rangle\langle-i\alpha|\right) \tag{9.1.3}$$

Para um desses casos, por exemplo, a distribuição a ser detectada por Bob quando este utiliza apenas bases corretas é dada por:

$$\begin{aligned}\langle X|\,\hat{\rho}_X\,|X\rangle &= \frac{1}{2}\left(|\langle X|\alpha\rangle|^2 + |\langle X|-\alpha\rangle|^2\right)\\ &= \frac{1}{\sqrt{2\pi}}\left[e^{-2(X-\alpha)^2} + e^{-2(X+\alpha)^2}\right]\end{aligned}$$

E, no caso extremo em que Eva interceptou todos os estados e enviou todos errados, Bob detectaria:

$$\begin{aligned}\langle X|\,\hat{\rho}_Y\,|X\rangle &= \frac{1}{2}\left(|\langle X|i\alpha\rangle|^2 + |\langle X|-i\alpha\rangle|^2\right)\\ &= \sqrt{\frac{2}{\pi}}e^{-2X^2}\end{aligned}$$

onde $\hat{X}\,|X\rangle = X\,|X\rangle$ e usamos a projeção dos estados coerentes sobre os estados "linha" $|X\rangle$ [7].

Estes são dois casos extremos dentre os quais a distribuição recebida por Bob sempre se situará: quando não há espionagem e quando o espião erra todos os estados enviados. Estas distribuições estão representadas na Figura 9.1.

Mais adiante, ao analisarmos nossa proposta de protocolo, definiremos uma quantidade simples M para medir a diferença entre as distribuições esperadas e efetivamente medidas por Bob (Seção 10.3.2) e, assim, quantificar os ataques de Eva.

9.1.3 Conclusão

A codificação da informação nas quadraturas de campos eletromagnéticos é possível devido às técnicas de produção de estados coerentes, deslocamento de fase e à detecção homódina. Esta codificação, feita em duas bases com dois estados cada, permite a detecção de espionagem devido à aleatoriedade das bases usadas, pois força um possível espião a errar a base em 50% das tentativas de medição, chegando a valores aleatórios para seus bits nestes casos e reenviando estados errados a Bob (ataque Intercepta-Reenvia). Eva, caso não queira se arriscar em sorteios, só poderá saber quais bases usar *após* a transmissão, quando então poderá medir quaisquer clones, sondas ou partes removidas do feixe, mas nunca o feixe na íntegra. Esta limitação de Eva é análoga àquela imposta pelo protocolo BB84 e é o que garante a detecção da espionagem e a transmissão de uma chave secreta. Entretanto, graças ao limiar de pós-seleção inexistente no BB84, o uso de estados coerentes da luz permite a transmissão por distâncias muito maiores, ou seja, canais muito mais atenuantes que os usados com estados de um fóton.

9.2 Protocolo H04

Nesta seção apresentaremos o protocolo proposto por Horak em 2004 [39]. Ele consiste de uma generalização, para estados comprimidos, do protocolo proposto por Namiki e Hirano [38], apresentado na seção anterior.

Repetiremos os passos do autor no cálculo de quantidades importantes e na análise de segurança para dois ataques: "Ataque por Medida Simultânea das Quadraturas" e "Ataque por Troca do Canal por Canal Superior". No capítulo seguinte faremos amplo uso dos resultados desta seção para a análise de segurança de nosso próprio protocolo, razão pela qual diversos resultados serão reobtidos.

9.2.1 Funcionamento do Protocolo

Inicialmente, Alice prepara um estado comprimido de mínima incerteza com amplitude α_0 e parâmetro de compressão r, ambos reais. A seguir, Alice aplica um *phase-shift* $\theta \in \{0, \pi/2, \pi, 3\pi/2\}$ no pulso. Cada *phase-shift* corresponde a um bit em uma determinada

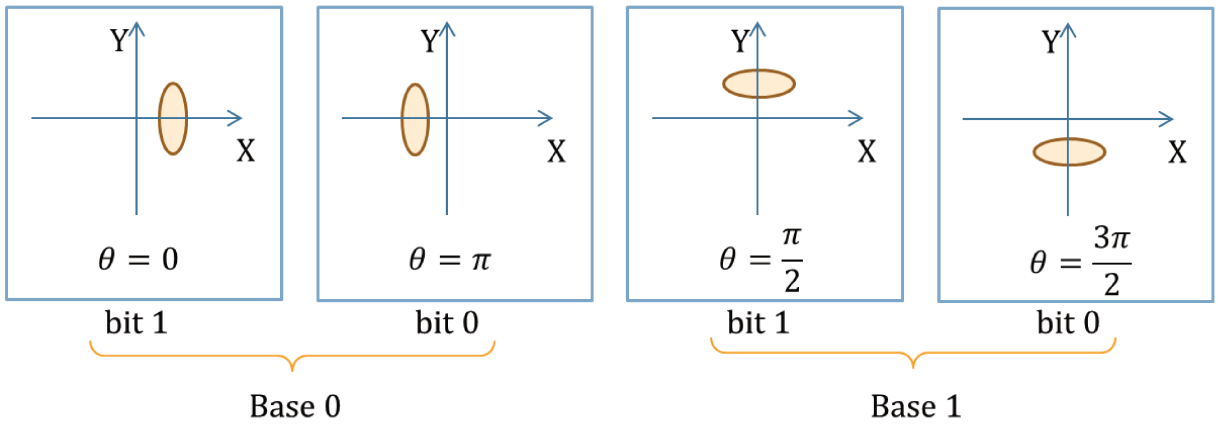


Figura 9.2: Estados utilizados pelo protocolo de Horak (H04).

base, conforme representado na Figura 9.2. Todos estes estados podem ser representados pelo ket geral:

$$|\psi_\theta\rangle = \underbrace{e^{\alpha_0 e^{i\theta}\hat{a}^\dagger - \alpha_0 e^{-i\theta}\hat{a}}}_{\hat{D}\left(\alpha_0 e^{i\theta}\right)} \underbrace{e^{\frac{1}{2}\left(re^{-2i\theta}\hat{a}^2 - re^{2i\theta}\hat{a}^{\dagger 2}\right)}}_{\hat{S}\left(re^{2i\theta}\right)} |0\rangle \tag{9.2.1}$$

$$\{\alpha_0, r\} \in \mathbb{R},\ \theta \in \left\{0, \frac{\pi}{2}, \pi, \frac{3\pi}{2}\right\}$$

Por fim, Alice envia estes pulsos a Bob. Nesta transmissão o pulso sofre atenuação, tanto por absorção do canal quanto pelas ações de espionagem. Em ambos os casos, a transmissão é modelada por um divisor de feixes com transmitância T e refletância R, de forma que $T^2 + R^2 = 1$.

O efeito do divisor de feixes pode ser descrito através da seguinte relação entre os operadores de modos de saída $\left(\hat{b}, \hat{b}^\dagger\right)$ e $\left(\hat{e}, \hat{e}^\dagger\right)$, correspondentes aos modos nos detectores de Bob e Eva, e os operadores de modos do sinal de entrada $\left(\hat{a}, \hat{a}^\dagger\right)$ e do vácuo $\left(\hat{v}, \hat{v}^\dagger\right)$:

$$\begin{pmatrix} \hat{b} \\ \hat{e} \end{pmatrix} = \begin{pmatrix} T & R \\ -R & T \end{pmatrix} \begin{pmatrix} \hat{a} \\ \hat{v} \end{pmatrix} \tag{9.2.2}$$

onde o sinal negativo é introduzido para que seja equacionada a diferença de fase criada entre as ondas transmitidas e refletidas pelo divisor.

Neste ponto, Horak acha conveniente expressar o estado transmitido através de sua função de distribuição de quasi-probabilidade de Wigner. Para isso podemos partir das funções de Wigner de entrada, já obtidas na Seção 6.3, [Eq. 6.3.1] e [Eq. 6.3.7], e utilizar a transformação do divisor de feixes, deduzida no Apêndice A.3, para funções de Wigner:

$$W(\beta,\epsilon) = W_{\alpha,\zeta}(T\beta - R\epsilon)\, W_{vác}(R\beta + T\epsilon) \tag{9.2.3}$$

As funções da direita são as funções de Wigner de entrada, calculadas sobre combinações das variáveis de saída. Na saída obtemos então:

$$W_\theta(\beta,\epsilon) = \frac{4}{\pi^2} e^{-2\left[e^{2r}\mathcal{R}(\alpha)^2 + e^{-2r}\mathcal{I}(\alpha)^2\right]} e^{-2\left(|R\beta+T\epsilon|^2\right)} \tag{9.2.4}$$

onde $\mathcal{R}$ e $\mathcal{I}$ tomam, respectivamente, as partes real e imaginária e

$$\alpha = (T\beta - R\epsilon)\, e^{-i\theta} - \alpha_0$$

No próximo passo, Bob sorteia aleatoriamente as bases em que fará suas medições. Se Bob escolhe a Base 1, Bob mede a parte real β_r (amplitude, equivalente à quadratura X) de sua variável β por detecção homódina. Se Bob escolhe a Base 0, Bob mede a parte imaginária β_i (fase, quadratura Y). Suas detecções seguem as distribuições de probabilidades:

$$P_\theta(\beta_r) = \int W_\theta(\beta,\epsilon)\, \mathrm{d}\beta_i \mathrm{d}\epsilon_r \mathrm{d}\epsilon_i \tag{9.2.5}$$

$$P_\theta(\beta_i) = \int W_\theta(\beta,\epsilon)\, \mathrm{d}\beta_r \mathrm{d}\epsilon_r \mathrm{d}\epsilon_i \tag{9.2.6}$$

Estas integrações são cálculos analíticos relativamente simples, pois utilizamos apenas as partes reais e imaginárias das variáveis complexas e a função de Wigner é real. Completamos os quadrados no expoente a cada integração, transformando a função a ser integrada em uma função gaussiana, cuja integral é bem conhecida. Para $\theta = 0$ temos:

$$P_0(\beta_r) = \sqrt{\frac{2}{\pi}} \frac{e^{-2\frac{(\beta_r - T\alpha_0)^2}{(T^2 e^{-2r} + R^2)}}}{\sqrt{T^2 e^{-2r} + R^2}} \tag{9.2.7}$$

$$P_0(\beta_i) = \sqrt{\frac{2}{\pi}} \frac{e^{-2\frac{\beta_i^2}{(T^2 e^{2r} + R^2)}}}{\sqrt{T^2 e^{2r} + R^2}} \tag{9.2.8}$$

Estas distribuições estão representadas na Figura 9.3, juntamente com uma visualização do estado $|\psi_0\rangle$ no plano das quadraturas $\beta_r \times \beta_i$ e uma interpretação da detecção homódina como sendo uma projeção do estado sobre o eixo de detecção.

Após a detecção, Bob verifica se seu resultado satisfaz a condição $|\beta_{r,i}| > \beta_c$, onde β_c é um valor limiar fixado para a pós-seleção. Caso esta condição não seja satisfeita, Bob diz a Alice para descartar seu bit. Caso a condição seja satisfeita, Bob atribui valor 1 para seu bit caso $\beta_{r,i} > \beta_c$ ou valor 0, caso $\beta_{r,i} < \beta_c$. O limiar de pós-seleção β_c tem o papel de reduzir as taxas

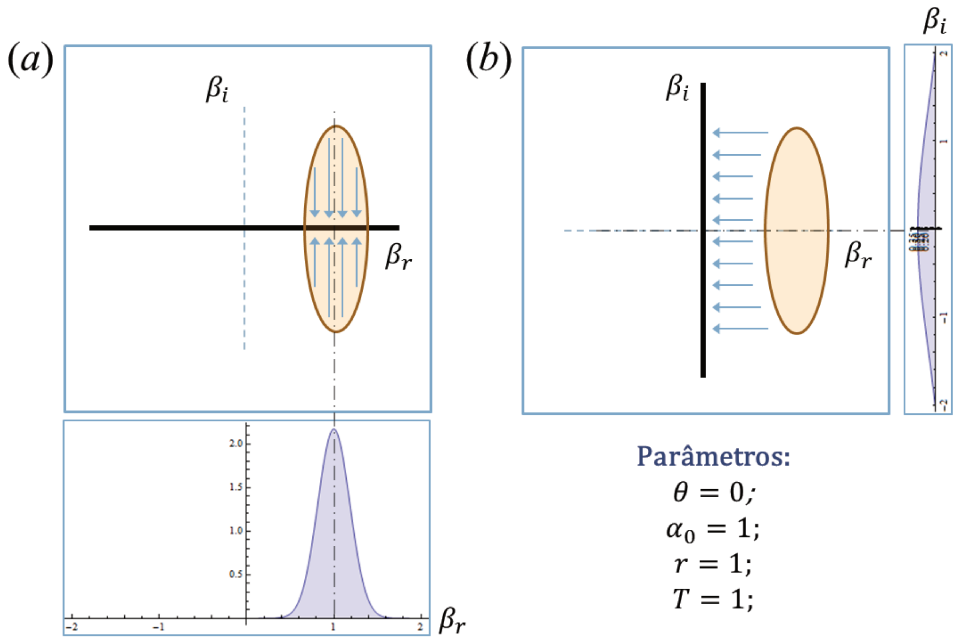


Figura 9.3: Distribuições de probabilidades obtidas por Bob ao receber o estado $|\psi_0\rangle$, (a) caso ele meça β_r ou (b) caso ele meça β_i. A detecção homódina projeta o estado sobre o eixo escolhido, gerando uma distribuição de probabilidades.

de erros mesmo para grandes sobreposições entre os estados, o que dificulta a espionagem.

Excluindo-se o intervalo $(-\beta_c, \beta_c)$, as probabilidades de que Bob meça bit 1 ou bit 0 são dadas por:

$$P(1) = \int_{\beta_c}^{\infty} P_0(\beta_r)\, \mathrm{d}\beta_r = \frac{1}{2} + \frac{1}{2}\Phi\left(\frac{\sqrt{2}\,(T\alpha_0 - \beta_c)}{\sqrt{T^2 e^{-2r} + R^2}}\right) \tag{9.2.9}$$

$$P(0) = \int_{-\infty}^{-\beta_c} P_0(\beta_r)\, \mathrm{d}\beta_r = \frac{1}{2} - \frac{1}{2}\Phi\left(\frac{\sqrt{2}\,(T\alpha_0 + \beta_c)}{\sqrt{T^2 e^{-2r} + R^2}}\right) \tag{9.2.10}$$

Onde $\Phi(x)$ é a função erro

$$\Phi(x) = \frac{2}{\sqrt{\pi}} \int_0^x e^{-t^2} \mathrm{d}t \tag{9.2.11}$$

9.2.2 Obtenção de Quantidades Importantes

Para facilitar o raciocínio, nas deduções a seguir consideraremos um *ensemble* de N estados transmitidos, todos com $\theta = 0$.

9.2.2.1 Taxa de bits aceitos

Após as N transmissões, o número de bits aceitos pela pós-seleção desses estados é dado por

$$N_{acc} = N_{\text{bits } 0} + N_{\text{bits } 1} = \frac{1}{2}N\int_{-\infty}^{-\beta_c} P_0\left(\beta_r\right)\mathrm{d}\beta_r + \frac{1}{2}N\int_{\beta_c}^{\infty} P_0\left(\beta_r\right)\mathrm{d}\beta_r = \frac{1}{2}N\left[P\left(0\right)+P\left(1\right)\right]$$

Onde o fator 1/2 aparece devido ao fato de Bob errar em 50% das vezes a base a ser usada, e descartar este bit.

9.2.2.2 Taxa de erros

A taxa de bits aceitos em relação ao total de estados transmitidos é

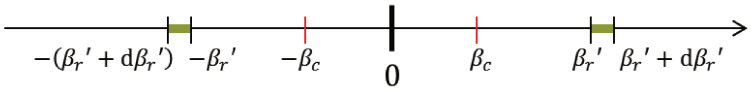
$$r_{acc} = \frac{N_{acc}}{N} = \frac{P\left(1\right)+P\left(0\right)}{2} \tag{9.2.12}$$

Se Alice enviou $\theta = 0$, Bob deveria ter obtido bit 1. Caso Bob obtenha bit 0, este bit está errado. A taxa de erros por bit aceito é dada por:

$$\delta = \frac{N_{\text{bits } 0}}{N_{acc}} = \frac{P\left(0\right)}{P\left(0\right)+P\left(1\right)} \tag{9.2.13}$$

9.2.2.3 Cálculo da informação mútua

Neste ponto consideraremos duas posições simétricas na reta β_r e descreveremos estas posições por um mesmo valor positivo β_r'.



Considerando apenas as medições não descartadas ($|\beta_r| > \beta_c$) e que resultaram β_r dentro de um intervalo $\left[-\left(\beta_r'+\mathrm{d}\beta_r'\right),-\beta_r'\right]$ ou $\left[\beta_r',\beta_r'+\mathrm{d}\beta_r'\right]$, o número de estados detectados por Bob é:

$$\mathrm{d}N\left(\beta_r'\right) = \frac{1}{2}NP_0\left(-\beta_r'\right)\mathrm{d}\beta_r' + \frac{1}{2}NP_0\left(\beta_r'\right)\mathrm{d}\beta_r'$$

Destas detecções, o número de medições erradas, para as quais $\beta_r \in \left[-\left(\beta_r'+\mathrm{d}\beta_r'\right),-\beta_r'\right]$, é:

$$\mathrm{d}N_{\text{bits } 0}\left(\beta_r'\right) = \frac{1}{2}NP_0\left(-\beta_r'\right)\mathrm{d}\beta_r'$$

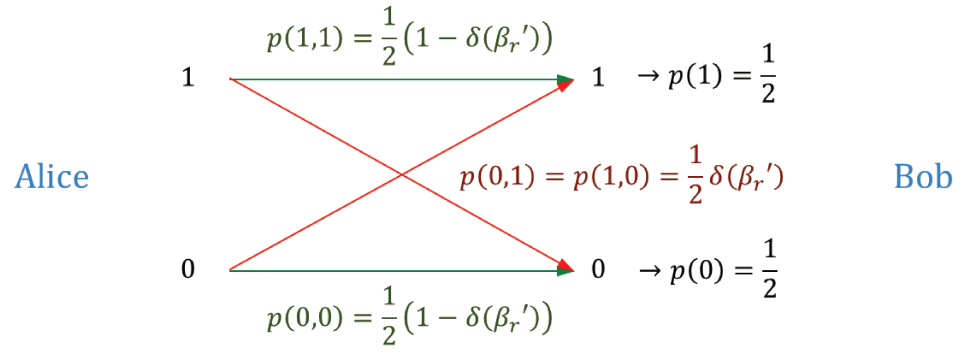


Figura 9.4: Modelagem do canal feita apenas para os bits aceitos. Para cada par de intervalos infinitesimais o canal é um canal binário simétrico.

Para os bits obtidos de medições que resultaram β_r dentro destes dois intervalos simétricos temos a taxa de erros:

$$\delta\left(\beta_r'\right) = \frac{\mathrm{d}N_{\text{bits }0}\left(\beta_r'\right)}{\mathrm{d}N\left(\beta_r'\right)} = \frac{P_0\left(-\beta_r'\right)}{P_0\left(-\beta_r'\right) + P_0\left(\beta_r'\right)} \tag{9.2.14}$$

Conforme a Figura 9.4, para cada par de intervalos infinitesimais o canal é um canal binário simétrico. Utilizamos então o resultado do Exemplo 1 da Seção 3.6 para o cálculo da informação mútua. O ganho de informações para cada bit obtido destes intervalos é dado por:

$$I\left(\beta_r'\right) = 1 + \delta\left(\beta_r'\right)\log_2\delta\left(\beta_r'\right) + \left[1 - \delta\left(\beta_r'\right)\right]\log_2\left[1 - \delta\left(\beta_r'\right)\right]$$

O total de informação trocada pelos estados medidos apenas nestes intervalos é dado por:

$$\mathrm{d}I\left(\beta_r'\right) = I\left(\beta_r'\right)\mathrm{d}N\left(\beta_r'\right) = I\left(\beta_r'\right)\frac{1}{2}N\left[P_0\left(-\beta_r'\right) + P_0\left(\beta_r'\right)\right]\mathrm{d}\beta_r'$$

Agora, obtemos o total de informações trocadas integrando em todo o domínio de β_r':

$$I_{Total} = \frac{1}{2}N\int_{\beta_c}^{\infty}\left[P_0\left(\beta_r'\right) + P_0\left(-\beta_r'\right)\right]\left\{1 + \delta\left(\beta_r'\right)\log_2\delta\left(\beta_r'\right) + \left[1 - \delta\left(\beta_r'\right)\right]\log_2\left[1 - \delta\left(\beta_r'\right)\right]\right\}\mathrm{d}\beta_r'$$

E o ganho médio de informação por bit aceito é:

$$I_{AB} = \frac{I_{Total}}{N_{acc}} = \int_{\beta_c}^{\infty}\mathrm{d}\beta_r\frac{P_0\left(\beta_r\right) + P_0\left(-\beta_r\right)}{P\left(0\right) + P\left(1\right)}\left\{1 + \delta\left(\beta_r\right)\log_2\delta\left(\beta_r\right) + \left[1 - \delta\left(\beta_r\right)\right]\log_2\left[1 - \delta\left(\beta_r\right)\right]\right\} \tag{9.2.15}$$

Onde retiramos o apóstrofe por conveniência.

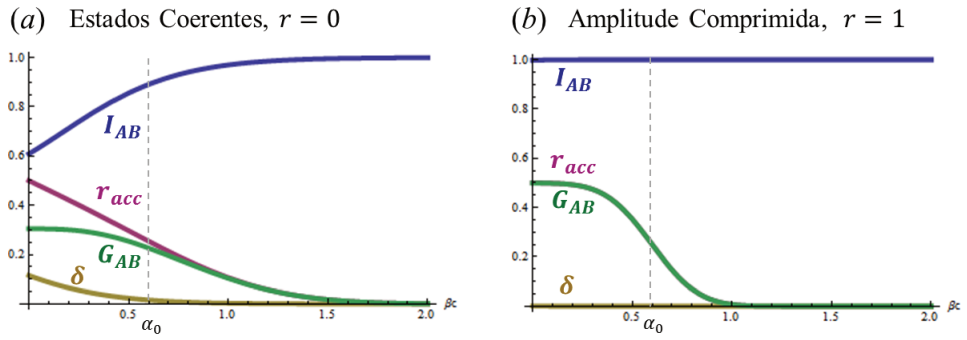


Figura 9.5: Representação da taxa de bits aceitos r_{acc}, taxa de erros por bit aceito δ, informação por bit aceito I_{AB} e ganho de informação média por estado transmitido G_{AB}, como função do limiar de pós-seleção, para (a) estados coerentes e (b) estados com amplitude comprimida ($r = 1$). A amplitude utilizada é $\alpha_0 = 0,6$ e o canal é sem perdas, $T = 1$.

9.2.2.4 Ganho médio de informação por estado transmitido

O ganho médio de informação por estado transmitido leva em conta a informação nula acrescida pelos estados descartados:

$$G_{AB} = r_{acc} I_{AB} \tag{9.2.16}$$

Como exemplo, na Figura 9.5 todas estas quantidades estão representadas como função do limiar de pós-seleção β_c para um estado coerente ($r = 0$) e um estado comprimido com parâmetro de compressão $r = 1$, para um canal sem perdas. Devido à compressão, os estados comprimidos são bem mais distinguíveis que os estados coerentes, carregando praticamente 1 bit de informação para cada bit aceito. Notamos claramente que no caso extremo em que o limiar excede a amplitude dos estados, $\beta_c > \alpha_0$, a taxa de bits aceitos cai abruptamente, pois uma região de grande probabilidade passa a ser excluída. Junto com esta taxa temos a queda do ganho médio de informações por estado transmitido. Isto implica que embora um incremento do limiar de pós-seleção aumente a informação por bit aceito (pois reduz a taxa de erros), o ganho médio de informações não acompanha este aumento, sofrendo uma redução (descarte de "medidas boas").

A solução lógica seria escolher $\beta_c = 0$, para que G_{AB} seja máxima. Porém, como veremos para os dois ataques a seguir, Eva obtém informações da chave crua, que depois terá de ser encurtada para dar origem à chave secreta. Quanto menor β_c, mais Eva conhecerá a chave e mais severa deverá ser a etapa de ampliação de privacidade. Este limiar é um parâmetro ajustável capaz de reduzir taxas de erros e as informações que um possível espião tem da chave crua, antes mesmo dos procedimentos públicos de purificação da chave.

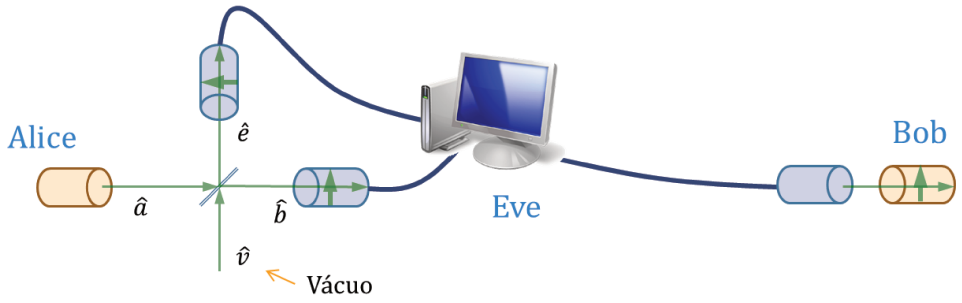


Figura 9.6: Ataque por medida simultânea das quadraturas. Eva se localiza imediatamente na saída do aparato de Alice (zero perdas), mede β_r na detecção homódina da direita e mede ϵ_i na detecção homódina de cima. A seguir, Eva decide qual estado será enviado e, através de um canal sem perdas (clássico), transmite essa informação ao emissor localizado imediatamente na entrada do detector de Bob (zero perdas).

9.2.3 Ataque por medida simultânea das quadraturas

Este é um ataque do tipo *intercepta-reenvia* (Seção 8.4.2), onde Eva recolhe todo o pulso de Alice e escolhe qual o melhor estado a ser gerado e enviado a Bob.

Funcionamento

Eva utiliza um divisor de feixes com $R^2 = T^2 = 1/2$ e realiza uma detecção homódina em cada saída, a fim de obter um par ordenado para cada pulso de entrada, conforme a Figura 9.6.

Sabendo a forma dos possíveis estados de Alice (devido à comunicação pública inicial), Eva utiliza o par ordenado para definir qual será o melhor estado a ser gerado. Eva divide o plano das quadraturas em regiões onde cada estado tem uma maior probabilidade de ser detectado do que os outros e assim, conforme a região em que um par ordenado é detectado, Eva escolhe qual estado vai gerar para Bob.

Se Eva mede a parte real da variável β e a parte imaginária da variável ϵ, Eva obtém a distribuição de probabilidade conjunta:

$$P_\theta\left(\beta_r, \epsilon_i\right) = \int W_\theta\left(\beta, \epsilon\right) \mathrm{d}\beta_i \mathrm{d}\epsilon_r \tag{9.2.17}$$

Que para todos os valores de parâmetros se fatoriza como $P_\theta\left(\beta_r, \epsilon_i\right) = P_\theta\left(\beta_r\right) P_\theta\left(\epsilon_i\right)$. Para os estados com $\theta = 0$ temos:

$$P_0\left(\beta_r, \epsilon_i\right) = P_0\left(\beta_r\right) P_0\left(\epsilon_i\right) = \frac{2}{\pi} \frac{e^{-2\frac{(\beta_r - T\alpha_0)^2}{(T^2 e^{-2r} + R^2)}}}{\sqrt{T^2 e^{-2r} + R^2}} \frac{e^{-2\frac{\epsilon_i^2}{(T^2 + R^2 e^{2r})}}}{\sqrt{T^2 + R^2 e^{2r}}} \tag{9.2.18}$$

Esta e as outras três distribuições de probabilidade conjunta estão representadas na Fi-

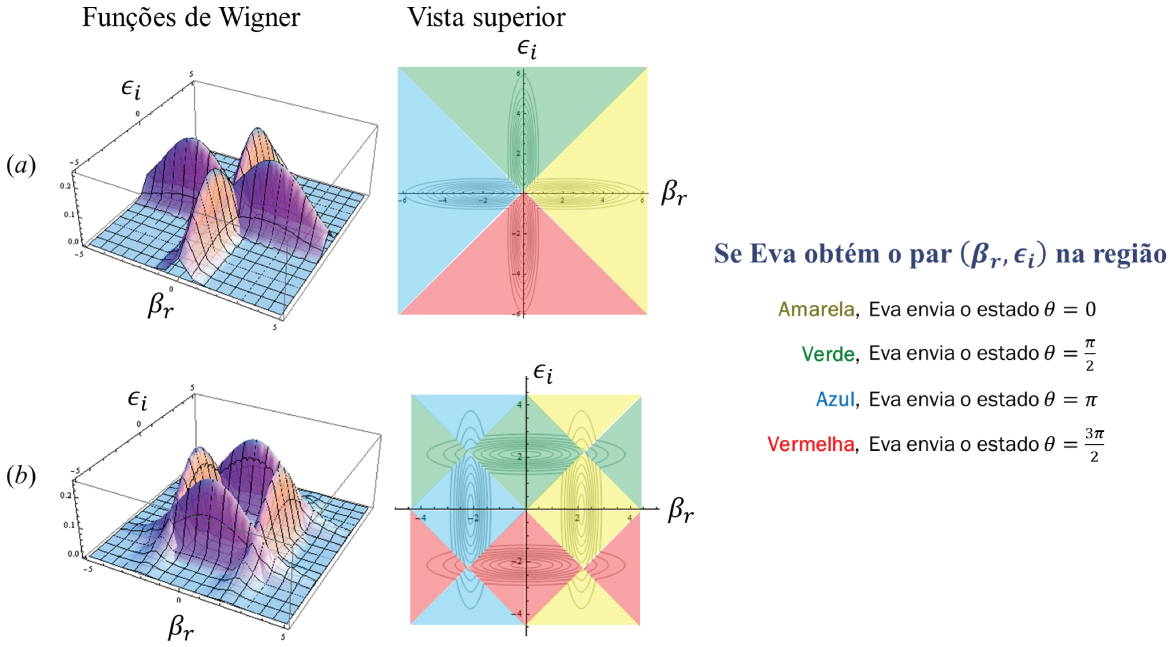


Figura 9.7: Gráfico das quatro distribuições de probabilidade conjunta para estados com (a) fase comprimida e (b) amplitude comprimida. Eva decide qual o melhor estado a enviar conforme a região em que sua medida se encontra. (Obs.: apenas um tipo de estado é transmitido por vez, aqui representamos os quatro tipos para visualização).

gura 9.7, juntamente com as regiões onde cada estado tem maior probabilidade de ser encontrado.

Detecção da Espionagem

Por simetria, em cada caso, a taxa de sucesso de Eva para este ataque pode ser calculada pela integral sobre a região amarela (região onde $P_0\left(\beta_r, \epsilon_i\right)$ é máxima):

$$p_{corr} = \int_A P_0\left(\beta_r, \epsilon_i\right) \mathrm{d}\beta_r \mathrm{d}\epsilon_i \tag{9.2.19}$$

No *paper* de Horak há um fator 2 devido ao fato de ser considerado apenas o primeiro quadrante.

Com este valor, Alice e Bob sabem que o número máximo de bits conhecidos por Eva será $N_{acc}p_{corr}$, quando Eva intercepta *todos* os pulsos. Esta é uma estimativa para as informações vazadas para Eva e indica o quanto Alice e Bob devem encurtar suas chaves no processo de ampliação de privacidade (caso tenham certeza de que este foi o ataque usado).

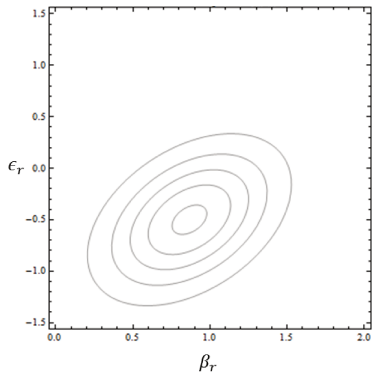


Figura 9.8: Gráfico de contornos da distribuição de probabilidades conjuntas $P_0(\beta_r, \epsilon_r)$ com $\alpha_0 = 1$, $r = 0,5$ e $T^2 = 0,75$, como obtido por Horak.

9.2.4 Ataque por troca do canal por Canal Superior

Neste ataque, Eva se aproveita de sua tecnologia superior e troca o canal ruidoso e extenuante, que Alice e Bob estavam usando, por um canal muito mais limpo. Desta forma, Eva pode separar a parte que seria perdida naturalmente na transmissão do pulso e realizar medições sobre ela, sem ser detectada. Com ainda mais tecnologia, Eva pode fazer uso de uma memória quântica, que armazena os estados até que as bases corretas sejam anunciadas por Alice. Eva então realiza todas as medições com as bases corretas, além de saber quais estados foram descartados.

Em sua parte dos pulsos, Eva pode realizar qualquer tipo de medição. Aqui consideraremos apenas o caso em que Eva mede a parte real de ϵ através de detecção homódina: medição de quadratura. A distribuição de probabilidade conjunta, detectada por Bob e Eva neste caso, é dada por:

$$P_\theta(\beta_r, \epsilon_r) = \int W_\theta(\beta, \epsilon)\, \mathrm{d}\beta_i \mathrm{d}\epsilon_i \tag{9.2.20}$$

$$P_0(\beta_r, \epsilon_r) = \frac{2}{\pi} e^r e^{-2\left[e^{2r}(T\beta_r - R\epsilon_r - \alpha_0)^2 + (R\beta_r + T\epsilon_r)^2\right]} \tag{9.2.21}$$

Para $r > 0$, esta distribuição está representada na Figura 9.8 e indica uma forte correlação entre as variáveis β_r e ϵ_r, ao contrário do que ocorre para os estados coerentes. Para 25% de perdas (divisão do sinal por Eva) é visível que a compressão na amplitude ajuda na ocultação da chave, pois quando Bob mede um valor relativamente alto para β_r, Eva tem grande probabilidade de obter um valor pequeno para ϵ_r. Desta forma, Bob pode elevar o limiar de pós-seleção, aumentando a taxa de erros de Eva e reduzindo a informação que Eva tem da chave.

Uma análise mais cuidadosa e esclarecedora deste ataque será feita para o protocolo que proporemos no próximo capítulo, nas Seções 10.4 e 10.5, onde faremos um tratamento um pouco diferente do de Horak.

9.2.5 Conclusão

Embora sua produção exija ainda avançados recursos tecnológicos, o uso de estados comprimidos da luz nos assegura um novo parâmetro de controle para o formato dos estados no espaço de fases. Esta liberdade pode ser usada em favor das partes comunicantes em um protocolo de criptografia, permitindo maiores taxas de transmissão de chave secreta através do uso de um limiar de pós-seleção. Horak destaca que mesmo uma pequena taxa de compressão, como $r = 0,5$, pode elevar a taxa máxima de transmissão de chave secreta em duas ordens de grandeza para perdas de 90% na transmissão. Para uma análise de segurança mais ampla deste protocolo, nos reportamos ao *paper* original de Horak [39].

Capítulo 10

Proposta de Um Novo Protocolo

Neste capítulo apresentaremos um novo protocolo com base nos conceitos introduzidos ao longo do texto. Em especial, uma boa compreensão da análise deste protocolo depende de uma leitura cuidadosa da seção anterior (protocolo H04), pois muitas das passagens são aplicações de conceitos apresentados naquela seção.

Considerando o fato de que a transmissão de informações pode ser feita por apenas dois estados, ponderando que quanto maior a sobreposição destes estados maior a taxa de erros (na ausência de um limiar de pós-seleção: $\beta_c = 0$) e buscando uma forma mais simples e imediata de detecção de espionagem, acreditamos que a introdução de pulsos isca, também nos protocolos de variáveis contínuas, seja uma boa opção.

Nosso protocolo consiste no uso de três estados comprimidos, dois deles a serem usados para a transmissão dos bits e um deles a ser usado como isca para a detecção e mensuração da espionagem, conforme representados na Figura 10.1.

Os estados de bit devem possuir uma sobreposição muito pequena entre si, de forma a serem completamente distinguíveis, permitindo baixíssimas taxas de erros na ausência de espionagem ou perdas pelo canal. Para isso, os estados são gerados equidistantes do eixo da quadratura Y e têm sua amplitude comprimida ($r > 0$).

O estado de isca, por outro lado, deve possuir o máximo de sobreposição possível com os estados de bit, de forma a confundir Eva de uma maneira mais eficaz. Fazemos então uma compressão de fase ($r_I < 0$) e o colocamos entre os estados de bit no plano das quadraturas.

O efeito de um limiar de pós-seleção será analisado apenas na Seção 10.5, seu objetivo é o de garantir a transmissão de uma chave secreta por distâncias maiores no caso de ataque por troca do canal por canal superior (entre outros).

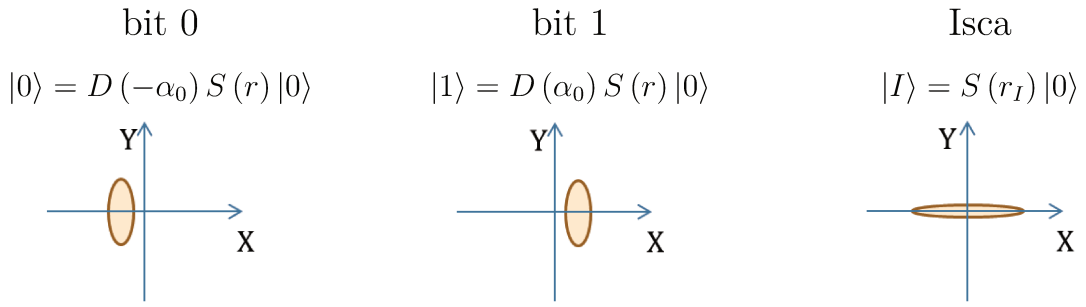


Figura 10.1: Representação dos três estados no plano das quadraturas. O estado de isca deve possuir grande sobreposição com os dois estados de bit, confundindo a análise de Eva. Para estes estados, $\alpha_0 > 0$, $r > 0$ e $r_I < 0$.

10.1 Funcionamento do Protocolo

Alice escolhe aleatoriamente entre os três estados representados na Figura 10.1, e os envia a Bob, anotando quais estados foram enviados e formando uma sequência de bits e iscas.

Como na Seção 9.2, as perdas pelo canal e a espionagem serão modeladas por um divisor de feixes e a descrição será feita através da função de Wigner.

Utilizando o resultado geral daquela seção para a função de Wigner de saída do divisor de feixes, [Eq. 9.2.4], obtemos a função de Wigner de cada estado:

$$\text{bit 0:}\quad W_{bit\,0}(\beta,\epsilon) = \tfrac{4}{\pi^2} e^{-2\left[e^{2r}(T\beta_r - R\epsilon_r + \alpha_0)^2 + e^{-2r}(T\beta_i - R\epsilon_i)^2\right]} e^{-2|R\beta + T\epsilon|^2}$$

$$\text{bit 1:}\quad W_{bit\,1}(\beta,\epsilon) = \tfrac{4}{\pi^2} e^{-2\left[e^{2r}(T\beta_r - R\epsilon_r - \alpha_0)^2 + e^{-2r}(T\beta_i - R\epsilon_i)^2\right]} e^{-2|R\beta + T\epsilon|^2}$$

$$\text{Isca:}\quad W_{Isca}(\beta,\epsilon) = \tfrac{4}{\pi^2} e^{-2\left[e^{2r_I}(T\beta_r - R\epsilon_r)^2 + e^{-2r_I}(T\beta_i - R\epsilon_i)^2\right]} e^{-2|R\beta + T\epsilon|^2}$$

Bob sempre fará a medição da parte real de sua variável β ("quadratura X"), pois é nela que toda a informação está codificada.

Ao final da transmissão, Alice diz a Bob quais estados eram iscas e Bob utiliza suas medidas para estes estados para obter uma estimativa da espionagem. Com os estados restantes (estados de bit), Alice e Bob constroem sua sequência de bits: Bob define seus bits como sendo bit 0, caso $\beta_r < 0$ ou bit 1, caso $\beta_r > 0$, para estes estados.

Os cálculos de Bob da estimativa da espionagem fornecem quanta informação foi vazada a Eva. Bob e Alice iniciam então os processos de correção de erros e ampliação de privacidade.

Um exemplo de transmissão com este protocolo está representado na Figura 10.2.

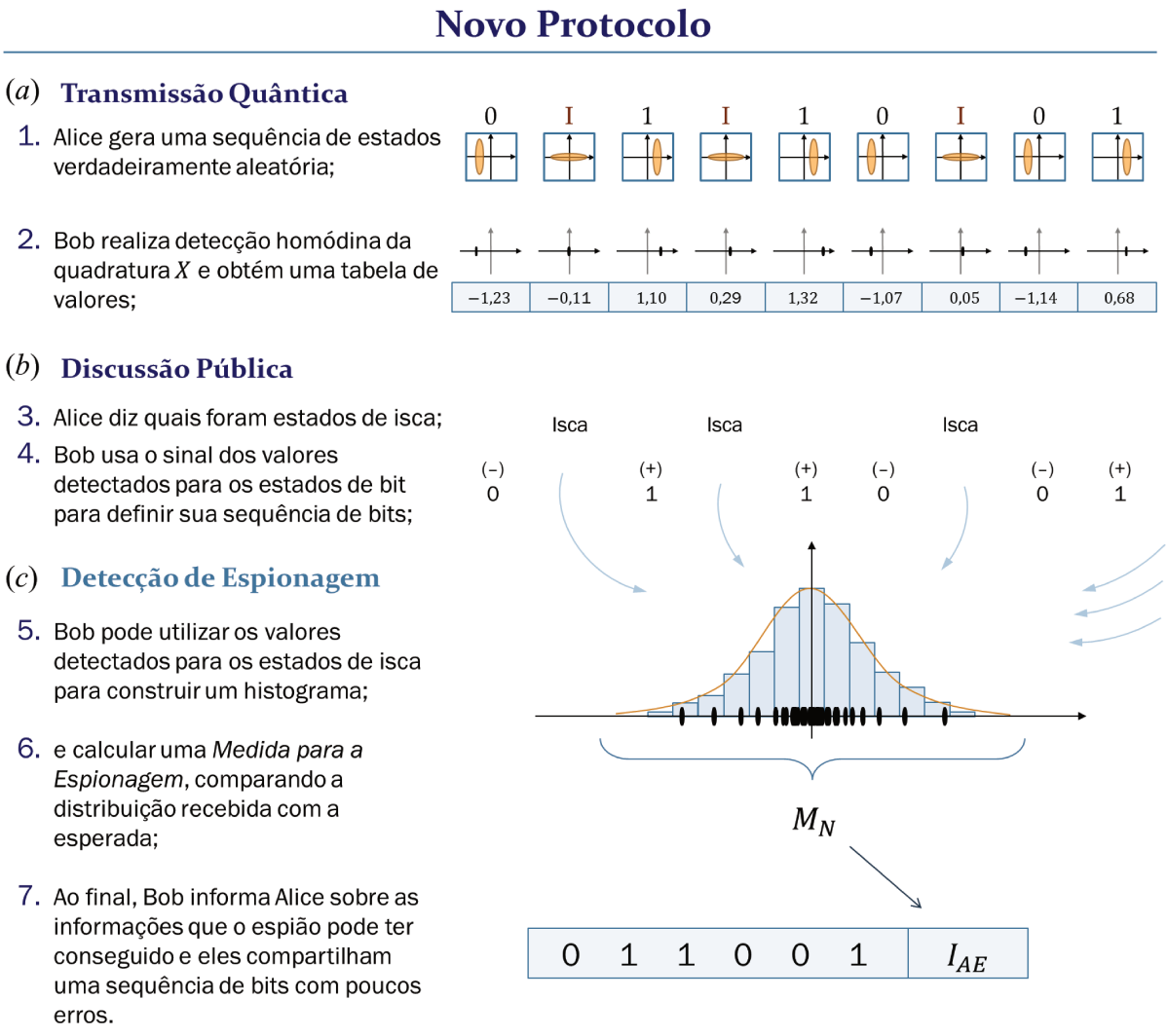


Figura 10.2: Exemplo de transmissão com o Novo Protocolo na ausência de espionagem ou perdas pelo canal: (*a*) Assim que cada pulso é enviado por Alice, ele deve ser detectado por Bob. Qualquer grande atraso pode também significar espionagem. (b) Em nenhum momento Bob ou Alice informam seus bits, Alice apenas indica quais são iscas e quais são bits. (c) Para uma longa transmissão, o histograma deve se aproximar de uma gaussiana, o formato esperado por Bob para a distribuição de suas medições. Como em todo protocolo de QKD, ao final Alice e Bob compartilham uma sequência muito parecida de bits e uma estimativa para as informações vazadas a Eva.

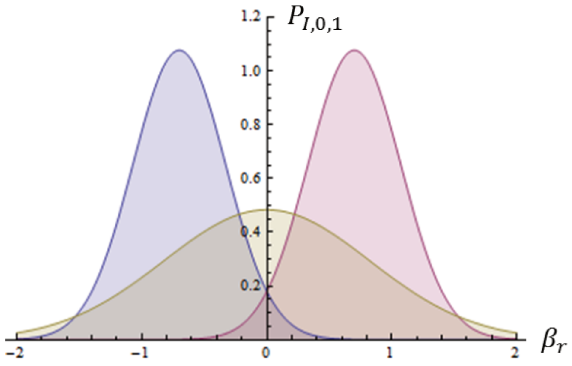


Figura 10.3: Comparação das três distribuições a serem recebidas por Bob. Os parâmetros são $\alpha_0 = 0.7$; $r = 0.3$; $r_I = -0.5$ e $T = 1$.

10.2 Quantidades Importantes

Caso Alice envie bit 1, Bob irá medir um determinado valor β_r com probabilidade:

$$P_1(\beta_r) = \int W_1(\beta, \epsilon)\, \mathrm{d}\beta_i \mathrm{d}\epsilon_r \mathrm{d}\epsilon_i = \sqrt{\frac{2}{\pi}} \frac{e^{-2\frac{(\beta_r - T\alpha_0)^2}{(T^2 e^{-2r} + R^2)}}}{\sqrt{T^2 e^{-2r} + R^2}} \tag{10.2.1}$$

Caso Alice envie bit 0, a distribuição recebida por Bob é simétrica à do bit 1:

$$P_0(\beta_r) = P_1(-\beta_r) \tag{10.2.2}$$

Por fim, se Alice envia o estado de Isca, Bob detecta:

$$P_I(\beta_r) = \int W_I(\beta, \epsilon)\, \mathrm{d}\beta_i \mathrm{d}\epsilon_r \mathrm{d}\epsilon_i = \sqrt{\frac{2}{\pi}} \frac{e^{-2\frac{\beta_r^2}{\left(T^2 e^{-2r_I} + R^2\right)}}}{\sqrt{T^2 e^{-2r_I} + R^2}} \tag{10.2.3}$$

Na ausência de espionagem, estas três distribuições estão representadas na Figura 10.3, para fins de visualização das sobreposições entre os estados.

Não havendo limiar de pós-seleção, as probabilidades que Bob tem de medir bit 1 ou bit 0 caso Alice envie bit 1 são dadas por:

$$P(1) = \int_0^\infty P_1(\beta_r)\, \mathrm{d}\beta_r = \frac{1}{2} + \frac{1}{2}\Phi\left(\frac{\sqrt{2}T\alpha_0}{\sqrt{T^2 e^{-2r} + R^2}}\right) \tag{10.2.4}$$

$$P(0) = \int_{-\infty}^0 P_1(\beta_r)\, \mathrm{d}\beta_r = \frac{1}{2} - \frac{1}{2}\Phi\left(\frac{\sqrt{2}T\alpha_0}{\sqrt{T^2 e^{-2r} + R^2}}\right) \tag{10.2.5}$$

onde $\Phi(x)$ é a função erro usual [Eq. 9.2.11].

10.2.1 Taxa de bits aceitos

Pela própria configuração do protocolo, todos os estados de bit são aceitos. Os estados de isca correspondem a 1/3 dos estados transmitidos, conforme o procedimento descrito aqui, mas podem ser escolhidos como uma fração menor ou maior. Em relação a todos os estados transmitidos, o número de estados que resultam em bits são:

$$r_{acc} = \frac{2}{3} \tag{10.2.6}$$

10.2.2 Taxa de erros

Se Alice enviou bit 1 e Bob obteve $\beta_r < 0$, Bob atribuiu valor 0 ao bit e este está errado. Da mesma forma o bit está errado se Alice envia bit 0 e Bob detecta $\beta_r > 0$. Como as distribuições são simétricas, podemos usar somente os resultados para quando Alice envia bit 1, e a taxa de erros por bit aceito é dada, para todos os bits aceitos, por:

$$\delta = P\left(0\right) \tag{10.2.7}$$

10.2.3 Cálculo da informação mútua

Novamente descreveremos posições opostas na reta β_r por um único valor positivo β_r', mas desta vez toda a reta β_r será considerada (sem limiar de pós-seleção).

Analogamente ao deduzido na Seção 9.2.2.3, a taxa de erros para os estados que resultarem em medições de β_r dentro dos intervalos infinitesimais $\left[-\left(\beta_r' + \mathrm{d}\beta_r'\right), -\beta_r'\right]$ ou $\left[\beta_r', \beta_r' + \mathrm{d}\beta_r'\right]$, deverá ser:

$$\delta\left(\beta_r'\right) = \frac{P_1\left(-\beta_r'\right)}{P_1\left(-\beta_r'\right) + P_1\left(\beta_r'\right)} \tag{10.2.8}$$

E para cada par destes intervalos o canal é um canal binário simétrico. O ganho de informação para cada bit proveniente destes intervalos é:

$$I\left(\beta_r'\right) = 1 + \delta\left(\beta_r'\right)\log_2\delta\left(\beta_r'\right) + \left[1 - \delta\left(\beta_r'\right)\right]\log_2\left[1 - \delta\left(\beta_r'\right)\right]$$

Fazendo uma média ponderada pela probabilidade de o bit ser proveniente de detecção nestes intervalos temos:

$$I_{AB} = \int_0^\infty \mathrm{d}\beta_r \left[P_1\left(\beta_r\right) + P_1\left(-\beta_r\right)\right]\left\{1 + \delta\left(\beta_r\right)\log_2\delta\left(\beta_r\right) + \left[1 - \delta\left(\beta_r\right)\right]\log_2\left[1 - \delta\left(\beta_r\right)\right]\right\} \tag{10.2.9}$$

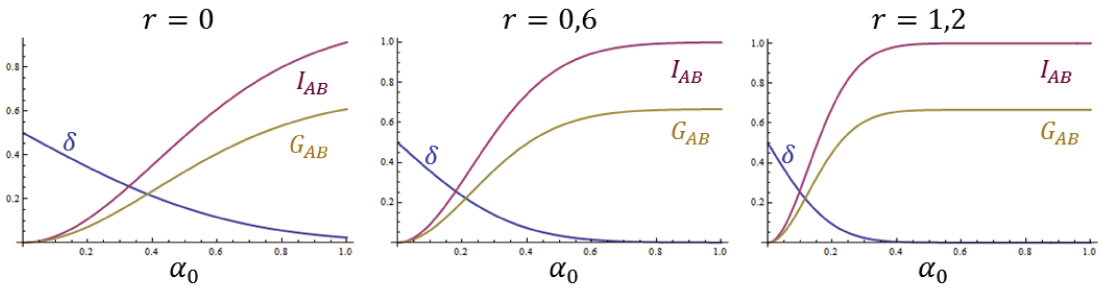


Figura 10.4: Representação da taxa de erros δ, informação I_{AB} por estado de bit transmitido e ganho de informação médio por estado transmitido G_{AB} como função dos parâmetros α_0 e r dos estados de bit. Aumentar r ou α_0 torna os estados de bit mais distintos, maximizando a informação que podem carregar. O canal é sem perdas, $T = 1$.

Onde retiramos o apóstrofe por conveniência. Este é o ganho de informação para cada estado de bit transmitido.

10.2.4 Ganho médio de informação por estado transmitido

Como apenas 2/3 dos estados são estados de bit, o ganho médio de informação por estado transmitido é:

$$G_{AB} = r_{acc} I_{AB} = \frac{2}{3} I_{AB} \tag{10.2.10}$$

Na Figura 10.4, estão representados a taxa de erros e o ganho de informação por estado de bit transmitido e o ganho de informação médio por estado transmitido, como funções do parâmetro α_0, para alguns valores de r (compressão na amplitude dos estados de bit). Quanto maior o valor de α_0 e r, mais distinguíveis são os estados de bit, levando rapidamente a informação ao máximo de 1 bit. Entretanto, um aumento exagerado destes parâmetros reduz a sobreposição destes estados com o estado de isca, permitindo que Eva realize ataques sem ser detectada. A combinação ideal de parâmetros pode ser procurada para cada ataque específico e na seção seguinte encontraremos a melhor combinação para a detecção do ataque por medida simultânea das quadraturas.

10.3 Ataque por medida simultânea das quadraturas

10.3.1 Funcionamento

Eva deve decidir qual estado foi enviado por Alice para que possa gerá-lo na entrada do detector de Bob. Utilizando um divisor de feixes com $R^2 = T^2 = 1/2$, Eva divide o feixe

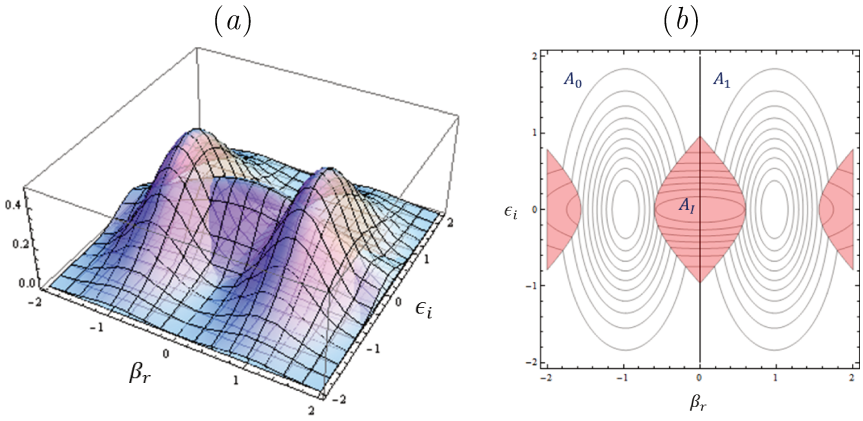


Figura 10.5: (a) Gráfico das três distribuições de probabilidade conjunta para os estados de bit 0, bit 1 e Isca (Obs.: apenas um tipo de estado é transmitido por vez, aqui representamos os três tipos para visualização). (b) Formato característico das regiões onde cada distribuição é dominante: A_0 - dominância do estado de bit 0; A_1 - dominância do estado de bit 1; A_I (região avermelhada) - dominância do estado de Isca. Eva decide qual o melhor estado a enviar conforme a região em que sua medida se encontra.

e realiza uma detecção homódina em cada metade. Obtendo o par ordenado (β_r, ϵ_i), Eva verifica nestas coordenadas qual das três distribuições (bit 0, bit 1 ou Isca) é maior, decidindo assim qual estado reproduzir para Bob. Estas três distribuições e as regiões onde cada uma delas é a maior estão representadas na Figura 10.5.

$$P_I(\beta_r, \epsilon_i) = P_I(\beta_r) P_I(\epsilon_i) = \frac{2}{\pi} e^{-r_I} \frac{e^{-2\frac{\beta_r^2 + e^{-2r_I}\epsilon_i^2}{\left(T^2 e^{-2r_I} + R^2\right)}}}{(T^2 e^{-2r_I} + R^2)} \tag{10.3.1}$$

$$P_0(\beta_r, \epsilon_i) = P_0(\beta_r) P_0(\epsilon_i) = \frac{2}{\pi} e^{-r} \frac{e^{-2\frac{(\beta_r + T\alpha_0)^2 + e^{-2r}\epsilon_i^2}{(T^2 e^{-2r} + R^2)}}}{(T^2 e^{-2r} + R^2)} \tag{10.3.2}$$

$$P_1(\beta_r, \epsilon_i) = P_1(\beta_r) P_1(\epsilon_i) = \frac{2}{\pi} e^{-r} \frac{e^{-2\frac{(\beta_r - T\alpha_0)^2 + e^{-2r}\epsilon_i^2}{(T^2 e^{-2r} + R^2)}}}{(T^2 e^{-2r} + R^2)} \tag{10.3.3}$$

10.3.2 Detecção da espionagem

Eva não é capaz de acertar o estado todas as vezes, e enviará a Bob uma fração de estados errados.

De posse dos resultados de suas medidas e sabendo quais são os estados de Isca, Bob pode separar os valores em dois grupos (bits ou Iscas) e fazer uma análise estatística para cada grupo. Para os estados de Isca, na ausência de espionagem ou perdas na transmissão,

a distribuição esperada por Bob para seu *ensemble* é dada pela [Eq. 10.2.3]:

$$P_{I(AB)}\left(\beta_r\right) = \sqrt{\frac{2}{\pi}} \frac{e^{-2\frac{\beta_r^2}{\left(T^2 e^{-2r_I} + R^2\right)}}}{\sqrt{T^2 e^{-2r_I} + R^2}} \tag{10.3.4}$$

Entretanto, Eva envia estados de bit algumas vezes, mesmo quando deveria enviar estados isca. As probabilidades que Eva tem de enviar cada tipo de estado, mesmo quando está recebendo apenas estados de isca, é:

$$P_{I\to 0} = \int_{A_0} P_I\left(\beta_r, \epsilon_i\right) \mathrm{d}\beta_r \mathrm{d}\epsilon_i \tag{10.3.5}$$

$$P_{I\to 1} = \int_{A_1} P_I\left(\beta_r, \epsilon_i\right) \mathrm{d}\beta_r \mathrm{d}\epsilon_i \tag{10.3.6}$$

$$P_{I\to I} = \int_{A_I} P_I\left(\beta_r, \epsilon_i\right) \mathrm{d}\beta_r \mathrm{d}\epsilon_i \tag{10.3.7}$$

onde as regiões A_0, A_1 e A_I estão representadas na Figura 10.5.*b*.

Dessa forma, Eva envia a Bob uma mistura de estados cuja distribuição a ser detectada é dada por:

$$P_{I(AEB)}\left(\beta_r\right) = P_{I\to 0} P_0\left(\beta_r\right) + P_{I\to 1} P_1\left(\beta_r\right) + P_{I\to I} P_I\left(\beta_r\right) \tag{10.3.8}$$

O formato típico das distribuições de probabilidade $P_{I(AB)}\left(\beta_r\right)$ e $P_{I(AEB)}\left(\beta_r\right)$ estão plotados na Figura 10.6.

Definimos agora uma *Medida da Espionagem* M, que irá quantificar a diferença entre as distribuições esperada e efetivamente recebida por Bob. Esta medida será escolhida como sendo a área entre os dois gráficos e será função dos três parâmetros do protocolo:

$$M\left(\alpha_0, r, r_I\right) = \int_{-\infty}^{\infty} \left| P_{I(AEB)}\left(\beta_r\right) - P_{I(AB)}\left(\beta_r\right) \right| \mathrm{d}\beta_r \tag{10.3.9}$$

Realizando uma maximização numérica de M em termos deste conjunto de parâmetros, descobrimos um máximo para os valores $\{\alpha_0 = 1.376, r = 0.765, r_I = -1.233\}$, para o ataque por medida simultânea das quadraturas:

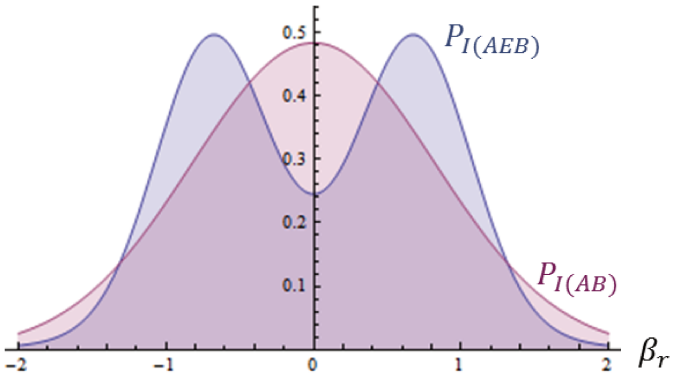


Figura 10.6: Comparação das distribuições teóricas a serem construídas por Bob a partir de suas detecções, na ausência de espionagem: $P_{I(AB)}$ (vermelha); e com espionagem por medida simultânea das quadraturas: $P_{I(AEB)}$ (azul). Em ambos os casos não há perdas no canal. Os parâmetros usados são $\alpha_0 = 0.7$; $r = 0.3$ e $r_I = -0.5$.

$$M\left(1.376, 0.765, -1.233\right) = M_{Máx} = 0.6627 \tag{10.3.10}$$

Para estes parâmetros, a taxa de erros na ausência de espionagem ou perdas pelo canal é baixíssima: $\delta = 1,67 \times 10^{-9}$. Por esta razão, e visando sermos capazes de detectar facilmente o ataque por medida simultânea das quadraturas, todos os tratamentos a seguir usarão estes parâmetros.

Na realidade, Bob só poderá obter M de forma numérica, pois seu conhecimento é apenas um conjunto de n_{total} valores numéricos reais β_r. Para isso, Bob precisa obter uma tabela para a distribuição recebida e outra tabela para a distribuição esperada, para que seja capaz de compará-las.

Bob pode, por exemplo, dividir o eixo β_r em N pequenos intervalos de tamanhos iguais Δ e contar o número de ocorrências n_i em cada um destes intervalos, de forma ordenada (negativo para positivo). Ao normalizar seus dados, Bob obtém a *distribuição discreta*:

$$p_i = \frac{n_i}{n_{total} \cdot \Delta} \tag{10.3.11}$$

onde $i < \frac{N}{2}$ corresponde aos dados com $\beta_r < 0$, por exemplo. Para comprovar a normalização desta distribuição fazemos:

$$\sum_{i=1}^{N} p_i \cdot \Delta = \frac{\Delta}{n_{total} \cdot \Delta} \sum_{i=1}^{N} n_i = \frac{n_{total}}{n_{total}} = 1$$

Com isto, para tabelar a distribuição $P_{I(AB)}\left(\beta_r\right)$, Bob pode simplesmente calcular seu valor em um ponto qualquer dentro de cada um destes N intervalos. Usando o ponto do meio dos

intervalos, a medida da diferença entre estas distribuições ("área entre os dois gráficos de barras") será dada por:

$$M_N = \Delta \cdot \sum_{i=1}^{N} \left| p_i - P_{I(AB)} \left(i \cdot \Delta - \frac{N+1}{2} \Delta \right) \right| \tag{10.3.12}$$

Exemplo

Neste exemplo mostraremos a validade do procedimento de Bob para a obtenção de M_N a partir de seus dados numéricos, comparando-o com o analítico M. Faremos uma simulação da espionagem de Eva caso ela decida medir apenas a parte β_r dos pulsos, ou seja, não utiliza um divisor de feixes. Naturalmente Bob não conhece o ataque a ser utilizado por Eva, razão pela qual é incapaz de escrever $P_{I(AEB)}(\beta_r)$ e calcular analiticamente o valor M, mas faremos este cálculo apenas para comparação e comprovação da validade do procedimento proposto.

Partindo diretamente das distribuições $P_0(\beta_r)$, $P_1(\beta_r)$ e $P_I(\beta_r)$ (Figura 10.3), Eva define os intervalos onde cada distribuição é dominante.

Para os parâmetros $\{\alpha_0 = 1.376;\ r = 0.765;\ r_I = -1.233\}$ temos cinco intervalos:

Intervalo	**Estado dominante**
$\beta_r < -1.908$	Isca
$-1.908 < \beta_r < -0.8953$	bit 0
$-0.8953 < \beta_r < 0.8953$	Isca
$0.8953 < \beta_r < 1.908$	bit 1
$\beta_r > 1.908$	Isca

Simulação Numérico - Computacional

- *Detecções de Eva*: A simulação inicia com a geração de 10^5 valores que obedecem à distribuição $P_I(\beta_r)$;
- *Análise de Eva*: Cada valor é separado conforme o intervalo que se encontra, definindo o uso de uma das três distribuições $P_I(\beta_r)$, $P_0(\beta_r)$ ou $P_1(\beta_r)$;
- *Detecções de Bob*: Um novo número aleatório é gerado conforme a distribuição definida por cada valor analisado;

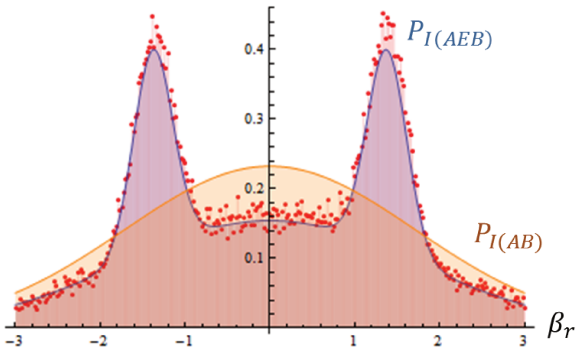


Figura 10.7: Simulação da transmissão de 10^5 pulsos isca com espionagem em todos. Em pontos vermelhos, histograma dos números de ocorrências de valores em $N = 300$ intervalos de largura $\Delta = 0.02$, normalizados para que a "área do gráfico" tenha valor unitário. Em azul, distribuição calculada analiticamente com o conhecimento do ataque. Em laranja, distribuição esperada na ausência de ataques.

- *Manipulação de Bob*: Com estes valores constrói-se a distribuição p_i, pelo procedimento descrito anteriormente, e calcula-se M_N.

Os pontos vermelhos na Figura 10.7 são os valores pontuais p_i da distribuição de probabilidades. Conhecendo p_i e calculando a função bem conhecida $P_{I(AB)}(\beta_r)$ dentro de cada intervalo, obtivemos

$$M_N = 0.4274$$

para esta simulação.

Analítico

Bob recebe uma mistura de estados com a distribuição [Eq. 10.3.8] e com os pesos:

$$P_{I\to 0} = \int_{-1.908}^{-0.8953} P_I(\beta_r)\,\mathrm{d}\beta_r = 0.1679 = P_{I\to 1}$$

$$P_{I\to I} = \left[\int_{-\infty}^{-1.908} + \int_{-0.8953}^{0.8953} + \int_{1.908}^{\infty}\right] P_I(\beta_r)\,\mathrm{d}\beta_r = 0,6643$$

Esta distribuição está plotada em azul na Figura 10.7, para este exemplo.

Desta vez, calculando a área entre os gráficos de $P_{I(AB)}(\beta_r)$ e $P_{I(AEB)}(\beta_r)$ obtemos:

$$M = 0.4354$$

indicando que a técnica numérica, para 10^5 pulsos, tem 98% de concordância com o

que poderia ser calculado caso Bob soubesse do ataque usado.

Como neste ataque Eva deve interceptar o pulso e realizar as medições antes de reproduzi-lo para Bob, Eva não poderá se aproveitar das comunicações clássicas posteriores à transmissão quântica, quando então Alice diz a Bob quais foram os estados de isca, para agir de forma seletiva com os pulsos. Por este motivo, para este ataque, Eva somente poderá reduzir o valor de M_N se interceptar apenas alguns dos pulsos e deixar que os outros sejam transmitidos a Bob sem interferência (não consideramos o uso de técnicas que envolvam emaranhamento). Para uma longa transmissão, reduzir linearmente o número de estados isca interceptados irá reduzir linearmente o valor de M_N, que é uma soma de termos. Se $M_N \approx M_{Máx}$, Eva terá medido *todos* os pulsos e se $M_N \approx 0$, Eva não terá medido *nenhum* pulso. Para os pulsos medidos, Eva terá a mesma taxa de erros que Bob teria, pois seu conjunto de pares ordenados para os estados de bit se reduzirá à distribuição esperada por Bob ao medir apenas β_r. A partir disso, obtemos a informação média que Eva acumulou da chave de Alice para cada estado de bit transmitido:

$$I_{AE} = \frac{M_N}{M_{Máx}} I_{AB} \tag{10.3.13}$$

Este valor multiplicado pelo número de bits transmitidos fornece o número mínimo de bits que Alice e Bob devem encurtar em suas chaves, com o fim de quase anular o conhecimento de Eva, durante a ampliação de privacidade (caso eles tenham certeza de que este foi o ataque realizado).

10.4 Ataque por troca do canal por Canal Superior

10.4.1 Funcionamento

Como Eva não pode ser detectada, pois se confunde com os ruídos, para este ataque só nos resta calcular a quantidade de informação que assumiremos que Eva adquiriu da chave.

Eva não necessita o uso de uma memória quântica para atacar otimamente este protocolo pois apenas uma base é usada. Para os estados de bit, as probabilidades conjuntas de medições de Eva e Bob são dadas por:

$$P_1(\beta_r, \epsilon_r) = \frac{2}{\pi} e^r e^{-2\left[e^{2r}(T\beta_r - R\epsilon_r - \alpha_0)^2 + (R\beta_r + T\epsilon_r)^2\right]} \tag{10.4.1}$$

$$P_0(\beta_r, \epsilon_r) = \frac{2}{\pi} e^r e^{-2\left[e^{2r}(T\beta_r - R\epsilon_r + \alpha_0)^2 + (R\beta_r + T\epsilon_r)^2\right]} \tag{10.4.2}$$

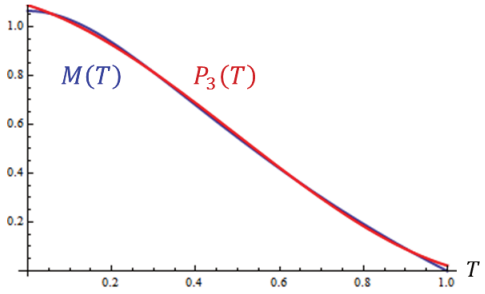


Figura 10.8: Em azul: Gráfico da Medida $M(T)$ para o ataque por troca do canal. Em vermelho: Aproximação com um polinômio de grau 3.

10.4.2 Detecção da Espionagem

Devido à alteração de todos os estados, que ao serem atenuados perdem compressão e se aproximam do estado de vácuo, podemos novamente definir uma medida da diferença entre a distribuição esperada e efetivamente detectada por Bob. Desta vez a diferença máxima possível ocorre quando Bob só recebe estados de vácuo e tem valor $M_{Máx} = M(T = 0) = 1.063$.

Como função da transmitância, o comportamento de $M(T)$ está plotado na Figura 10.8 e pode ser aproximado com boa precisão por um polinômio de grau 3:

$$M(T) = 1,087 - 0,5298T - 1,604T^2 + 1,069T^3 \tag{10.4.3}$$

Com esta expressão simples, partindo dos dados experimentais, Bob calcula uma estimativa para $M(T)$ e obtém uma aproximação para T.

Observemos agora que há uma simetria entre as distribuições recebidas por Eva e Bob neste ataque (para os três tipos de estados):

$$P_{Eva}(T, R, \epsilon_r) = P_{Bob}(R, T, -\beta_r) \tag{10.4.4}$$

As distribuições recebidas por Bob para diferentes taxas de atenuação estão representadas na Figura 10.9.*a*. Na Figura 10.9.*b* observamos o comportamento das distribuições conjuntas de probabilidades. Um aumento na taxa de atenuação "rotaciona" as distribuições, permitindo que Eva seja cada vez mais capaz de distinguir os estados a partir de medições de ϵ_r. Por outro lado, para pequenas atenuações (grande T), quanto mais Bob está certo sobre uma de suas medições, menos Eva conhece sobre o estado.

Devido à simetria das distribuições, podemos calcular a informação que Eva tem de cada bit da chave da mesma forma que fizemos para Bob, a partir das equações [Eq. 10.2.1] a [Eq. 10.2.9]. Uma comparação entre a informação que Eva e Bob têm da chave em função

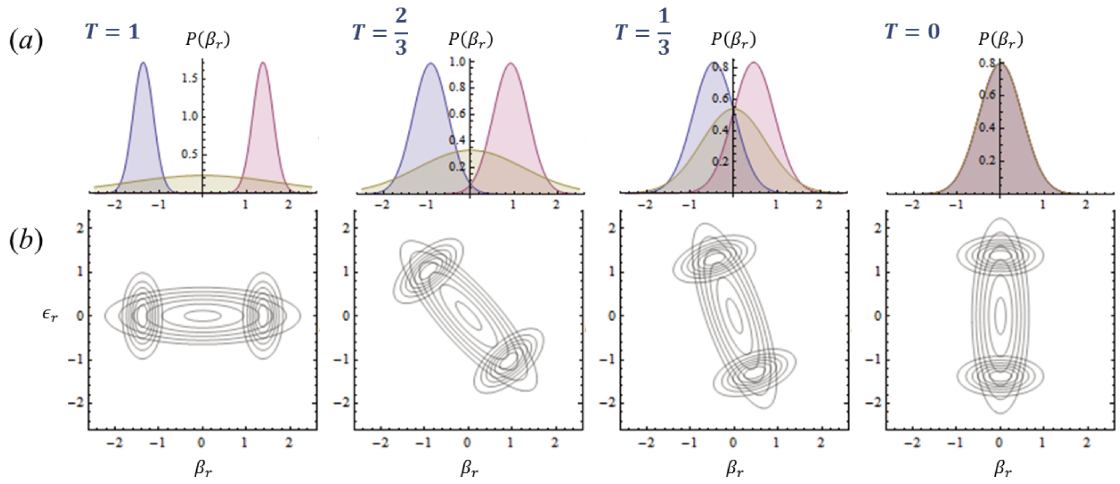


Figura 10.9: (a) Gráficos das três distribuições de probabilidades recebidas por Bob - $P_0(\beta_r)$ (azul), $P_1(\beta_r)$ (vermelho) e $P_I(\beta_r)$ (amarelo), e (b) Gráficos de contornos das três distribuições de probabilidades conjuntas - $P_{0,1,I}(\beta_r, \epsilon_r)$, para quatro diferentes transmitâncias. As distribuições recebidas por Bob se aproximam da distribuição do vácuo quanto menor a taxa de transmissão. Os parâmetros dos estados foram os ajustados para maximizar a detecção do ataque por medida simultânea de quadraturas: $\alpha_0 = 1,376$, $r = 0,765$ e $r_I = -1,233$.

da transmitância, neste caso, está plotada na Figura 10.11.a.

Considerando o cenário paranóico, a partir do valor calculado para M_N, Bob calcula a informação de Eva para diversos tipos de ataques e adota o maior valor para o cálculo do número de bits a serem encurtados na chave durante a ampliação de privacidade.

10.5 Reintrodução de um Limiar de Pós-seleção

A introdução de um limiar de pós-seleção corresponde à exclusão de uma faixa vertical na região central dos gráficos de contorno da Figura 10.9.b. Esta exclusão altera a forma da distribuição (renormalizada) construída por Eva e, portanto, suas informações sobre a chave. Considerando-se apenas os bits aceitos, a nova distribuição recebida por Eva é:

$$P_{Eva\ 0,1}(\epsilon_r) = \frac{1}{\mathcal{N}_{0,1}} \left[\int_{-\infty}^{-\beta_c} + \int_{\beta_c}^{\infty} \right] P_{0,1}(\beta_r, \epsilon_r)\, \mathrm{d}\beta_r \tag{10.5.1}$$

onde o fator de normalização $\mathcal{N}$ é dado por:

$$\mathcal{N}_{0,1} = \int_{-\infty}^{\infty} \left[\int_{-\infty}^{-\beta_c} + \int_{\beta_c}^{\infty} \right] P_{0,1}(\beta_r, \epsilon_r)\, \mathrm{d}\beta_r \mathrm{d}\epsilon_r \tag{10.5.2}$$

As distribuições construídas por Eva para os estados de bit aceitos estão plotadas na

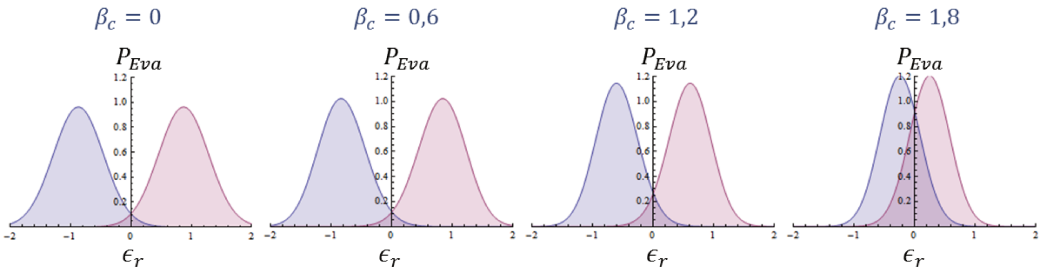


Figura 10.10: Distribuições construídas por Eva para os estados de bit 1 (azul) e bit 0 (vermelho), para diversos limiares de pós-seleção β_c quando $T = \sqrt{0.6}$. As medidas de Eva descartadas pelo limiar de pós-seleção fazem com que as distribuições *renormalizadas* para os dados restantes se aproximem, dificultando a distinção entre os estados e, portanto, reduzindo a informação de Eva.

Figura 10.10 para alguns valores de pós-seleção.

Por analogia com a Seção 10.4, escrevemos:

$$P(1) = \int_{-\infty}^{0} P_{Eva\ 1}(\epsilon_r)\, \mathrm{d}\epsilon_r \tag{10.5.3}$$

$$P(0) = \int_{0}^{\infty} P_{Eva\ 1}(\epsilon_r)\, \mathrm{d}\epsilon_r \tag{10.5.4}$$

onde explicitamos o efeito da rotação das probabilidades (Figura 10.9.b) trocando os índices de integração (ao inverso de Bob, Eva deve obter bit 1 se $\epsilon_r < 0$ e bit 0 se $\epsilon_r > 0$).

10.5.1 Taxa de erros nos bits de Eva

O limiar de pós-seleção está embutido apenas na distribuição recebida por Eva, de forma que todas as quantidades a seguir são expressões idênticas às da Seção 10.4. Como a distribuição calculada para Eva já está normalizada temos:

$$\delta = P(0) \tag{10.5.5}$$

10.5.2 Cálculo da informação de Eva

A expressão para a informação mútua por bit aceito torna-se (distribuição de Eva já normalizada):

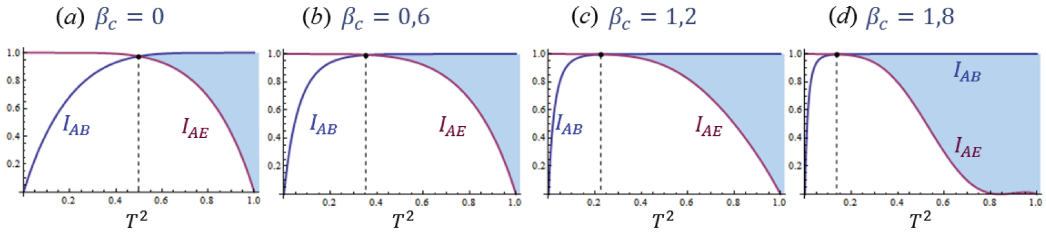


Figura 10.11: Gráfico da informação por bit aceito, em função de T^2, de Bob (azul) e Eva (vermelho). (a) A simetria entre as funções $I_{AB}(T)$ e $I_{AE}(T)$ foi desmascarada pelo reescalonamento do eixo T para T^2 (quando não há limiar de pós-seleção). (b), (c), e (d) O efeito de um limiar de pós-seleção é o de maximizar as informações que Alice e Bob têm da chave e reduzir a informação de Eva.

$$I_{AE} = \int_0^\infty \mathrm{d}\epsilon_r \left[P_{Eva\ 1}(\epsilon_r) + P_{Eva\ 1}(-\epsilon_r)\right] \left\{1 + \delta(\epsilon_r)\log_2\delta(\epsilon_r) + \left[1-\delta(\epsilon_r)\right]\log_2\left[1-\delta(\epsilon_r)\right]\right\} \tag{10.5.6}$$

onde

$$\delta(\epsilon_r) = \frac{P_{Eva\ 1}(-\epsilon_r)}{P_{Eva\ 1}(-\epsilon_r) + P_{Eva\ 1}(\epsilon_r)} \tag{10.5.7}$$

O comportamento das informações por bit aceito de Bob e Eva está representado na Figura 10.11 para alguns parâmetros de pós-seleção. Uma redução gradual da taxa de transmissão reduz a diferença $I_{AB} - I_{AE}$ e, a partir do ponto crítico $I_{AB} = I_{AE}$, não é mais possível a transmissão de uma chave secreta, pois a espiã possui mais informações da chave que o destinatário. O valor da transmitância neste ponto é um limitante para a comunicação, mas pode ser deslocado através do limiar de pós-seleção β_c: quanto maior β_c, menor transmitância mínima requerida. Esta característica é herdada do protocolo de Horak, pois os estados de bit são os mesmos, bem como a idéia da pós-seleção.

10.6 Conclusão

Diferentemente do protocolo B92, nosso protocolo faz uso de dois estados praticamente ortogonais para a codificação dos bits e a não-ortogonalidade exigida para a segurança da transmissão é inserida através de um novo estado, o estado de Isca. Esta configuração permite baixíssimas taxas de erros na ausência de espionagem e/ou quando o canal é de qualidade razoável (poucas perdas). Em uma consideração mais realista, demonstramos que a partir das estatísticas de detecção geradas pela transmissão dos estados Isca, é possível a detecção da espionagem e o cálculo da informação vazada para um possível espião para dois tipos de

ataques.

Partindo dos mesmos dados experimentais, a consideração de um ou outro tipo de ataque leva a diferentes estimativas para as informações que Eva tem da chave. Por esta razão, em um cenário paranóico, consideramos que Eva realiza o melhor tipo de ataque possível: aquele que retira mais informações da chave e é mais difícil de ser detectado. Dessa forma, após a consideração de vários tipos de ataques, supomos que Eva realizou aquele ataque que lhe garantiu a maior dentre as informações calculadas e tomamos este valor como estimativa a ser usada na ampliação de privacidade.

Devido à simetria inerente à ação do divisor de feixes (uma troca de Bob por Eva leva praticamente ao mesmo esquema), na ausência de um limiar de pós-seleção, a transmissividade do canal deve ser maior que $T = \sqrt{1/2} \approx 0.71$ para que seja possível a troca de chaves secretas. O efeito do limiar de pós-seleção é forçar Eva a excluir seus melhores dados à respeito da chave, enquanto Alice e Bob excluem a pior parte de seus dados. Esta quebra de simetria entre as distribuições detectadas por Bob e Eva aumenta a diferença $I_{AB} - I_{AE}$, relacionada ao comprimento máximo da chave secreta, de forma que o protocolo possa tolerar menores taxas de transmissão pelo canal (ou ataques mais agressivos).

Embora tenhamos provado que este protocolo é seguro contra estes dois ataques específicos, uma prova geral de segurança requer a análise de estratégias de espionagem consideradas ideais para este protocolo. Atualmente, certas estratégias de ataque foram sugeridas como ideais para alguns protocolos com variáveis contínuas e algumas delas propõem a clonagem dos feixes transmitidos através de emaranhamento [39]. A análise de tais tipos de ataques é deixada para trabalhos futuros.

Conclusões Finais

Ao longo deste trabalho salientamos o importante papel histórico representado pela criptografia e pela criptanálise. Acreditamos que um estudo proveitoso da criptografia quântica não pode ser levado a cabo sem o conhecimento das motivações para o seu desenvolvimento e do funcionamento das cifras clássicas mais famosas. Conhecer a estrutura destas cifras parece fornecer um guia de raciocínio durante a análise dos protocolos de distribuição quântica de chaves (QKD), facilitando sua compreensão. Muitos procedimentos clássicos podem ainda ser utilizados na criptografia quântica. Dentre eles temos a autenticação do remetente, a correção de erros e a ampliação de privacidade.

As motivações para a criação de um protocolo baseado em estados comprimidos foram várias:

- O uso de estados de um fóton, além da dificuldade de produção, impõe limitações nas distâncias de operação, fatores que são melhorados com o uso de estados contínuos;
- Quando estados comprimidos interagem com o vácuo em um divisor de feixes, as duas saídas possuem correlações. Estas correlações garantem um aumento na taxa de bits seguros quando realizamos uma pós-seleção [39];
- Por fim, os estados comprimidos da luz fornecem um grau de liberdade extra para a moldagem da forma dos estados no plano das quadraturas, possibilitando a criação de inúmeros novos protocolos, talvez mais vantajosos em certos aspectos.

A análise deste protocolo foi toda baseada na descrição dos estados através da função de Wigner, um tratamento não convencional descoberto no *paper* de Horak [39]. Esta abordagem se mostrou bastante conveniente, pois permitiu visualizações simples dos estados e suas transformações durante os ataques, além de originar de forma direta as distribuições mensuráveis.

Analisamos com cuidado o efeito de um limiar de pós-seleção dos resultados e realçamos sua ação destrutiva sobre as informações que um possível espião possa ter adquirido da chave.

Por fim, concluímos que o limiar de pós-seleção, o parâmetro de compressão e a amplitude dos campos utilizados são as três entidades chave para a otimização da transmissão segura

por um canal atenuante. Com elas, aumentamos a sobreposição entre os estados usados, para dificultar sua distinção, e ainda assim obtemos baixas taxas de erros.

Apêndice A

Teoremas e Resultados Úteis

A.1 Teorema da Expansão de um Operador

A expansão em série de Taylor de uma função $f(x)$, infinitamente diferenciável, ao redor de um determinado valor a é dada pela expressão

$$f(x) = \sum_{n=0}^{\infty} \frac{f^{(n)}(a)}{n!} (x-a)^n \tag{A.1.1}$$

Suponha agora que um operador $\hat{f}(x)$, função contínua e diferenciável da variável x, seja composto por dois operadores $\hat{A}$ e $\hat{B}$ na forma [6]:

$$\hat{f}(x) = e^{x\hat{A}} \hat{B} e^{-x\hat{A}} \tag{A.1.2}$$

Queremos fazer sua expansão em série de Taylor ao redor de $x = 0$. Calculando sua primeira derivada em relação a x temos:

$$\frac{\mathrm{d}\hat{f}(x)}{\mathrm{d}x} = e^{x\hat{A}} \hat{A} \hat{B} e^{-x\hat{A}} - e^{x\hat{A}} \hat{B} \hat{A} e^{-x\hat{A}} = e^{x\hat{A}} \left[\hat{A}, \hat{B}\right] e^{-x\hat{A}} \tag{A.1.3}$$

Calculando esta derivada em $x = 0$, temos:

$$\hat{f}'(0) = \left[\hat{A}, \hat{B}\right] \tag{A.1.4}$$

Prosseguindo com o cálculo de derivadas de ordem superior encontramos um padrão simples, em que a derivada seguinte, calculada em 0, é o comutador do operador $\hat{A}$ com a derivada anterior calculada em 0. Com este padrão obtemos uma fórmula para a expansão de uma função de dois operadores $\hat{A}$ e $\hat{B}$ na forma $e^{x\hat{A}} \hat{B} e^{-x\hat{A}}$:

$$e^{x\hat{A}}\hat{B}e^{-x\hat{A}} = \hat{B} + x\left[\hat{A},\hat{B}\right] + \frac{x^2}{2}\left[\hat{A},\left[\hat{A},\hat{B}\right]\right] + \frac{x^3}{3!}\left[\hat{A},\left[\hat{A},\left[\hat{A},\hat{B}\right]\right]\right] + ... \tag{A.1.5}$$

Quando o comutador $\left[\hat{A},\hat{B}\right] = c$, um número complexo, todos os termos da série além do segundo termo se anulam e temos:

$$e^{x\hat{A}}\hat{B}e^{-x\hat{A}} = \hat{B} + cx \tag{A.1.6}$$

Ou seja, o operador $e^{x\hat{A}}$ atua com uma translação sobre o operador $\hat{B}$. Como exemplos temos o caso em que $\hat{B} = \hat{q}$ e $\hat{A} = i\hat{p}/\hbar$ e também o operador deslocamento de Glauber, quando $x = 1$, $\hat{A} = \alpha^*\hat{a} - \alpha\hat{a}^\dagger$, $\hat{B} = \hat{a}$ ou $\hat{B} = \hat{a}^\dagger$, onde $\hat{a}$ e $\hat{a}^\dagger$ são os operadores de aniquilação e criação.

A.2 Teorema de Campbell-Baker-Hausdorff

Sejam $\hat{A}$ e $\hat{B}$ dois operadores que não necessariamente comutam, mas que

$$\left[\hat{A},\left[\hat{A},\hat{B}\right]\right] = 0 = \left[\hat{B},\left[\hat{A},\hat{B}\right]\right] \tag{A.2.1}$$

O teorema de Campbell-Baker-Hausdorff diz que para estes operadores:

$$e^{x\left(\hat{A}+\hat{B}\right)} = e^{x\hat{A}}e^{x\hat{B}}e^{-\frac{x^2}{2}\left[\hat{A},\hat{B}\right]} = e^{x\hat{B}}e^{x\hat{A}}e^{\frac{x^2}{2}\left[\hat{A},\hat{B}\right]} \tag{A.2.2}$$

Uma prova para este teorema pode ser feita como se segue [6]:
Vamos definir um novo operador $\hat{C}(x)$ como

$$\hat{C}(x) \equiv e^{x\hat{A}}e^{x\hat{B}} \tag{A.2.3}$$

Tomando sua derivada com relação a x temos:

$$\begin{aligned}
\frac{\mathrm{d}\hat{C}(x)}{\mathrm{d}x} &= \hat{A}e^{x\hat{A}}e^{x\hat{B}} + e^{x\hat{A}}\hat{B}e^{x\hat{B}} \\
&= \hat{A}e^{x\hat{A}}e^{x\hat{B}} + e^{x\hat{A}}\hat{B}e^{-x\hat{A}}e^{x\hat{A}}e^{x\hat{B}} \\
&= \left\{\hat{A} + e^{x\hat{A}}\hat{B}e^{-x\hat{A}}\right\}\hat{C}(x) \\
&= \left\{(\hat{A}+\hat{B}) + x\left[\hat{A},\hat{B}\right]\right\}\hat{C}(x)
\end{aligned} \tag{A.2.4}$$

Onde usamos a expressão para expansão de um operador [Eq. A.1.5] e o fato de que os comutadores de ordens maiores são nulos [Eq. A.2.1]. Os componentes $\left(\hat{A}+\hat{B}\right)$ e $x\left[\hat{A},\hat{B}\right]$

do termo entre chaves podem ser ordenados arbitrariamente, já que comutam.

Outra organização possível dos termos durante a derivada seria:

$$\begin{aligned}\frac{\mathrm{d}\hat{C}(x)}{\mathrm{d}x} &= e^{x\hat{A}}\hat{A}e^{x\hat{B}} + e^{x\hat{A}}e^{x\hat{B}}\hat{B} \\ &= \hat{C}(x)\left\{e^{-x\hat{B}}\hat{A}e^{x\hat{B}} + \hat{B}\right\} \\ &= \hat{C}(x)\left\{\hat{A} + x\left[\hat{A},\hat{B}\right] + \hat{B}\right\} \\ &= \hat{C}(x)\left\{\left(\hat{A}+\hat{B}\right) + x\left[\hat{A},\hat{B}\right]\right\} \end{aligned} \tag{A.2.5}$$

Desta forma, concluímos que os operadores $\hat{C}(x)$ e $\left\{\hat{A}+\hat{B}+x\left[\hat{A},\hat{B}\right]\right\}$ comutam e podemos integrar a equação [Eq. A.2.4] em relação a x como uma equação diferencial ordinária:

$$\int \frac{\mathrm{d}\hat{C}(x)}{\hat{C}(x)} = \int \left\{\left(\hat{A}+\hat{B}\right) + x\left[\hat{A},\hat{B}\right]\right\}\mathrm{d}x$$

$$\hat{C}(x) = e^{x\hat{A}}e^{x\hat{B}} = e^{x\left(\hat{A}+\hat{B}\right)+\frac{x^2}{2}\left[\hat{A},\hat{B}\right]} = e^{x\left(\hat{A}+\hat{B}\right)}e^{\frac{x^2}{2}\left[\hat{A},\hat{B}\right]}$$

Como pode ser verificado por diferenciação direta.

A.3 Transformação das funções de Wigner pelo Divisor de Feixes

Nesta seção iremos obter uma expressão não trivial que relaciona as funções de Wigner de entrada e saída de um divisor de feixes. Esta relação foi descoberta em um *paper* publicado por Wu [40] e deduzida a partir do ponto de partida indicado no *paper* de Ou *et al.* [41].

A transformação do divisor de feixes sobre os operadores de modos de entrada é dada por

$$\begin{pmatrix}\hat{b}\\ \hat{e}\end{pmatrix} = \begin{pmatrix}T & R\\ -R & T\end{pmatrix}\begin{pmatrix}\hat{a}\\ \hat{v}\end{pmatrix} \tag{A.3.1}$$

O ponto de partida é o requerimento de que o valor esperado de uma função $f\left(\hat{b},\hat{e}\right)$, quando calculado sobre $\hat{\rho}_{out}$, deve ser igual ao valor esperado correspondente calculado sobre $\hat{\rho}_{in}$ quando a função é escrita em termos dos operadores de entrada [41]:

$$\mathbf{Tr}\left[f\left(\hat{b},\hat{e}\right)\hat{\rho}_{out}\right] = \mathbf{Tr}\left[f\left(T\hat{a}+R\hat{v}, -R\hat{a}+T\hat{v}\right)\hat{\rho}_{in}\right] \tag{A.3.2}$$

A função $f\left(\hat{b},\hat{e}\right)$ é uma função geral, escrita em termos dos operadores de modos de saída

e seus conjugados. Sendo a relação válida para uma $f\left(\hat{b},\hat{e}\right)$ qualquer, assumimos que esta função seja um produto de operadores deslocamento $D\left(\mu\right)D\left(\eta\right)$ com ordenamento simétrico, sendo o primeiro operador escrito em termos dos operadores $\hat{b}$ e $\hat{b}^{\dagger}$ e o segundo em termos de $\hat{e}$ e $\hat{e}^{\dagger}$:

$$f\left(\hat{b},\hat{e}\right)=e^{\mu\hat{b}^{\dagger}-\mu^{*}\hat{b}}e^{\eta\hat{e}^{\dagger}-\eta^{*}\hat{e}}=D\left(\mu\right)D\left(\eta\right)$$

Imediatamente reconhecemos a função característica de dois modos, definida na Seção 6.4:

$$\chi\left(\mu,\eta\right)=\mathbf{Tr}\left[D\left(\mu\right)D\left(\eta\right)\hat{\rho}_{out}\right]=\mathbf{Tr}\left[D\left(T\hat{a}+R\hat{v}\right)D\left(-R\hat{a}+T\hat{v}\right)\hat{\rho}_{in}\right] \tag{A.3.3}$$

Tentaremos agora separar os operadores da direita na forma de um produto de operadores deslocamento, onde cada um esteja escrito em termos de apenas um operador de modo e seu conjugado. Lembrando que os operadores $\hat{a}$ e $\hat{v}$ se referem a modos distintos e comutam e fazendo uso do teorema de Campbell-Baker-Hausdorff (Apêndice A.2) para separar as exponenciais, temos:

$$\begin{aligned}D\left(T\hat{a}+R\hat{v}\right)D\left(-R\hat{a}+T\hat{v}\right) &= e^{\mu\left(T\hat{a}^{\dagger}+R\hat{v}^{\dagger}\right)-\mu^{*}\left(T\hat{a}+R\hat{v}\right)}e^{\eta\left(-R\hat{a}^{\dagger}+T\hat{v}^{\dagger}\right)-\eta^{*}\left(-R\hat{a}+T\hat{v}\right)}\\ &= e^{T\left(\mu\hat{a}^{\dagger}-\mu^{*}\hat{a}\right)+R\left(\mu\hat{v}^{\dagger}-\mu^{*}\hat{v}\right)}e^{-R\left(\eta\hat{a}^{\dagger}-\eta^{*}\hat{a}\right)+T\left(\eta\hat{v}^{\dagger}-\eta^{*}\hat{v}\right)}\\ &= e^{T\left(\mu\hat{a}^{\dagger}-\mu^{*}\hat{a}\right)}e^{R\left(\mu\hat{v}^{\dagger}-\mu^{*}\hat{v}\right)}e^{-R\left(\eta\hat{a}^{\dagger}-\eta^{*}\hat{a}\right)}e^{T\left(\eta\hat{v}^{\dagger}-\eta^{*}\hat{v}\right)}\end{aligned}$$

Queremos agora reagrupar as exponenciais com os operadores de mesmo modo (1ª com 3ª e 2ª com 4ª). Fazemos novamente uso do teorema de Campbell-Baker-Hausdorff. As relações de comutação são:

$$\left[T\left(\mu\hat{a}^{\dagger}-\mu^{*}\hat{a}\right),-R\left(\eta\hat{a}^{\dagger}-\eta^{*}\hat{a}\right)\right]=-RT\mu\eta^{*}+RT\mu^{*}\eta$$

$$\left[R\left(\mu\hat{v}^{\dagger}-\mu^{*}\hat{v}\right),T\left(\eta\hat{v}^{\dagger}-\eta^{*}\hat{v}\right)\right]=RT\mu\eta^{*}-RT\mu^{*}\eta$$

Que, por serem contantes, comutam com cada expoente satisfazendo a condição do teorema. Temos então:

$$\begin{aligned}D\left(T\hat{a}+R\hat{v}\right)D\left(-R\hat{a}+T\hat{v}\right) &= e^{\left(T\mu-R\eta\right)\hat{a}^{\dagger}-\left(T\mu-R\eta\right)^{*}\hat{a}}e^{\left(R\mu+T\eta\right)\hat{v}^{\dagger}-\left(R\mu+T\eta\right)^{*}\hat{v}}\\ &= D\left(T\mu-R\eta\right)D\left(R\mu+T\eta\right)\end{aligned} \tag{A.3.4}$$

Onde o primeiro operador deslocamento está escrito em termos de $\hat{a}$ e $\hat{a}^{\dagger}$ e o segundo em

termos de $\hat{v}$ e $\hat{v}^{\dagger}$.

Devido à montagem, os estados de entrada são independentes e separáveis:

$$\hat{\rho}_{in} = \hat{\rho}_{\alpha,\zeta} \otimes \hat{\rho}_{vác} \tag{A.3.5}$$

Assim, podemos agrupá-los convenientemente:

$$\chi(\mu,\eta) = \mathbf{Tr}\left[D(T\mu - R\eta)\,\hat{\rho}_{\alpha,\zeta} \otimes D(R\mu + T\eta)\,\hat{\rho}_{vác}\right]$$

e como estes operadores atuam em espaços diferentes, o traço do produto é o produto dos traços:

$$\chi(\mu,\eta) = \mathbf{Tr}\left[D(T\mu - R\eta)\,\hat{\rho}_{\alpha,\zeta}\right]\mathbf{Tr}\left[D(R\mu + T\eta)\,\hat{\rho}_{vác}\right] \tag{A.3.6}$$

Agora utilizaremos a definição da função de Wigner a partir da função característica para obtermos a função de Wigner de saída:

$$\begin{aligned} W(\beta,\epsilon) &= \frac{1}{\pi^4}\int\int \mathrm{d}^2\mu\mathrm{d}^2\eta e^{(\beta\mu^* - \beta^*\mu)} e^{(\epsilon\eta^* - \epsilon^*\eta)}\chi(\mu,\eta) \\ &= \frac{1}{\pi^4}\int\int \mathrm{d}^2\mu\mathrm{d}^2\eta e^{(\beta\mu^* - \beta^*\mu)} e^{(\epsilon\eta^* - \epsilon^*\eta)}\mathbf{Tr}\left[D(T\mu - R\eta)\,\hat{\rho}_{\alpha,\zeta}\right]\mathbf{Tr}\left[D(R\mu + T\eta)\,\hat{\rho}_{vác}\right] \end{aligned}$$

Com o fim de separar estas integrais introduzimos a mudança de variáveis:

$$\begin{pmatrix} \lambda \\ \xi \end{pmatrix} = \begin{pmatrix} T & -R \\ R & T \end{pmatrix}\begin{pmatrix} \mu \\ \eta \end{pmatrix} \Rightarrow \begin{pmatrix} \mu \\ \eta \end{pmatrix} = \begin{pmatrix} T & R \\ -R & T \end{pmatrix}\begin{pmatrix} \lambda \\ \xi \end{pmatrix} \tag{A.3.7}$$

Esta transformação tem jacobiano unitário, implicando em conservação do volume:

$$\mathrm{d}^2\mu\mathrm{d}^2\eta = \mathrm{d}^2\lambda\mathrm{d}^2\xi \tag{A.3.8}$$

As integrais então se tornam:

$$\begin{aligned} &= \frac{1}{\pi^4}\int\int \mathrm{d}^2\lambda\mathrm{d}^2\xi e^{\beta(T\lambda+R\xi)^* - \beta^*(T\lambda+R\xi)} e^{\epsilon(-R\lambda+T\xi)^* - \epsilon^*(-R\lambda+T\xi)}\mathbf{Tr}\left[D(\lambda)\,\hat{\rho}_{\alpha,\zeta}\right]\mathbf{Tr}\left[D(\xi)\,\hat{\rho}_{vác}\right] \\ &= \frac{1}{\pi^2}\int e^{(T\beta - R\epsilon)\lambda^* - (T\beta - R\epsilon)^*\lambda}\mathbf{Tr}\left[D(\lambda)\,\hat{\rho}_{\alpha,\zeta}\right]\mathrm{d}^2\lambda \cdot \frac{1}{\pi^2}\int e^{(R\beta+T\epsilon)\xi^* - (R\beta+T\epsilon)^*\xi}\mathbf{Tr}\left[D(\xi)\,\hat{\rho}_{vác}\right]\mathrm{d}^2\xi \end{aligned}$$

Reconhecemos as funções de Wigner de entrada e obtemos finalmente a relação:

$$W(\beta,\epsilon) = W_{\alpha,\zeta}(T\beta - R\epsilon)\, W_{vác}(R\beta + T\epsilon) \tag{A.3.9}$$

Referências Bibliográficas

[1] Tkotz, V. **Criptografia - Segredos Embalados para Viagem**, São Paulo: Editora Novatec, 2005. 355p.

[2] Singh, S. **The Code Book**: The Science of Secrecy from Ancient Egypt to Quantum Cryptography. New York: Anchor Books, 2000. 432p.
Uma curta entrevista com Leonard Adleman pode ser encontrada no CD de acompanhamento, disponível para download gratuito no site do autor <http://www.simonsingh.net/Code_Book_Download.html>

[3] Hughes, R.J.; Alde, D.M.; Dyer, P.; Luther, G.G.; Morgan, G.L.; Schauer, M. Quantum Cryptography. **Contemp. Phys**, v.36, p. 149-163, 1995. - Disponível em
<http://arxiv.org/PS_cache/quant-ph/pdf/9504/9504002v1.pdf>

[4] Grindlay, B. **Quantum Cryptography** - A study into the present technologies and future applications, Next Generation Security Software, 2003. - Disponível em
<http://www.scribd.com/doc/29473417/Quantum-Cryptography-A-Study-Into-Present-Technologies-and-Future-Applications-sflb>

[5] Scully, M.O.; Sargent III, M. The concept of the photon, **Physics Today**, p. 329-338, Mar 1972.

[6] Mandel, L.; Wolf, E. **Optical Coherence And Quantum Optics**. Cambridge: Cambridge Un. Press, 1995. 1166p. - Chap. 11, p.522-572.

[7] Loudon, R.; Knight, P.L. Squeezed States. **Journal Of Modern Optics**, v.34, nos. 6/7, p. 709-759, 1987.

[8] Shannon, C.E., 1949, A Mathematical Theory Of Communication, **Bell Syst. Tech. J.** v.27, n.4, p. 379-423, 623–656, Jul/Oct 1948.

[9] Shannon, C.E., 1949, Communication Theory of Secrecy Systems, **Bell Syst. Tech. J.** v.28, n.4, p. 656-715, 1949.

[10] Scully, M.O.; Zubairy, M.S. **Quantum Optics**. Cambridge: Cambridge Un. Press, 1997. 630p. - Sec. 4.4.2, p.125-131.

[11] Glauber, R.J. Coherent and Incoherent States of the Radiation Field. **Phys. Rev.** v.131, n.6, p. 2766–2788, Sep 1963.

[12] Cahill, K.E.; Glauber, R.J. Ordered Expansions in Boson Amplitude Operators. **Phys. Rev.** v.177, n.5, p.1857-1881, Jan 1969.

[13] Cahill, K.E.; Glauber, R.J. Density Operators and Quasiprobability Distributions. **Phys. Rev.** v.177, n.5, p.1882-1902, Jan 1969.

[14] Hillery, M.; O'Connell, R.F.; Scully, M.O.; Wigner, E.P. Distribution Functions In Physics: Fundamentals. **Physics Reports**, v.106, n.3, p.121-167, 1984.

[15] Schleich, W.P. **Quantum Optics In Phase Space**. Berlin: Wiley-VCH, 2001. 695p. - Chaps. 2-4, p.35-151.

[16] Ekert, A.K.; Huttner, B.; Palma, G.M.; Peres, A. Eavesdropping on Quantum-Cryptographical Systems. **Physical Review A**, v.50, n.2, p.1047-1056, 1994.

[17] Cover, T.M; Thomas, J.A. **Elements Of Information Theory**. 2nd ed. Hoboken: John Wiley and Sons, 2006. 748p. - Chaps. 1-2, p.13-55.

[18] Stix, G. Best-Kept Secrets – "Unbreakable Quantum Encryption Has Arrived", **Scientific American** - Jan 2005. p.79

[19] SECOQC **White Paper on Quantum Key Distribution and Cryptography**, Jan 2007. - Disponível em <http://www.secoqc.net/downloads/secoqc_crypto_wp.pdf>

[20] Aharonov, Y.; Bohm, D. Significance of electromagnetic potentials in the quantum theory, **Phys. Rev.** v.115, n.3, p. 485-491, Aug 1959.

[21] Tonomura, A.; Matsuda, T.; Suzuki, R.; Fukuhara, A.; Osakabe, N.; Umezaki, H.; Endo, J.; Shinagawa, K.; Sugita, Y.; Fujiwara, H. Observation of Aharonov-Bohm effect by electron holography, **Phys. Rev. Lett.** v.48, n.21, p. 1443-1446, May 1982.

[22] Jackson, J.D. **Classical Electrodynamics**. 3rd ed. Hoboken: John Wiley and Sons, 1999. - Sec. 6.3.

[23] Walls, D.F.; Milburn, G.J. **Quantum Optics**. 2nd ed. Berlin: Springer-Verlag, 2008. 425p. - Sec. 5.2.4.

[24] Dirac, P.M. **The Principles of Quantum Mechanics**. 4th ed. Oxford: Oxford University Press, 1967. 314p. - Sec. 21

[25] Aguiar, M.A.M. **Tópicos de Mecânica Clássica**. Nov 2010. - Notas de aula na página do autor
<http://www.ifi.unicamp.br/~aguiar/top-mec-clas.pdf>

[26] Griffiths, D.J. **Introduction To Quantum Mechanics**. Upper Saddle River: Prentice Hall, 1995. 394p. - Sec. 2.3.

[27] Reif, F. **Fundamentals of Statistical and Thermal Physics**. New York: McGraw-Hill Book Company, 1965. 651p.

[28] Harris, T. How File Compression Works, **HowStuffWorks.com**, Jan 2001. - Disponível em
<http://www.howstuffworks.com/file-compression.htm>

[29] Wiesner, S. Conjugate Coding, **ACM SIGACT News**, v.15, n.1, p.78-88, 1983. - Disponível em
<http://portal.acm.org/citation.cfm?id=1008908.1008920>

[30] Pasquinucci, A. **A first Glimpse at Quantum Cryptography**, UCCI.IT, 2004. (GNU Free Document) - Disponível em
<http://www.ucci.it/docs/QC-First_Glimpse-0.5.pdf>

[31] Bennett, C.H.; Brassard, G. Quantum Cryptography: Public Key Distribution and Coin Tossing. **Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing**, Bangalore, India, (IEEE, New York), 1984. p. 175. - Disponível em
<http://www.research.ibm.com/people/b/bennetc/bennettc198469790513.pdf>

[32] Dusek, M.; Lütkenhaus, N.; Hendrych, M. Quantum Cryptography. **E. Wolf, Progress In Optics**, 199X. - Disponível em
<http://arxiv.org/PS_cache/quant-ph/pdf/0601/0601207v3.pdf>

[33] Brassard, G. Brief History of Quantum Cryptography: A Personal Perspective, **Workshop On Theory and Practice in Information-Theoretic**

Security. IEEE Information Theory, Oct 2005. - Disponível em <http://arxiv.org/PS_cache/quant-ph/pdf/0604/0604072v1.pdf>

[34] Rigolin, G.; Rieznick, A. A. Introdução à criptografia quântica, **Revista Brasileira de Ensino de Física**, v.27, n.4, p. 517-526, Out 2005.

[35] Smolin, J. A., The early days of experimental quantum cryptography, **IBM J. Res. & Dev.** v.48, n.1, Jan 2004.

[36] Bennett, C.H. Quantum cryptography using any two nonorthogonal states, **Phys. Rev. Lett.** v.68, n.21, p. 3121-3124, May 1992.

[37] Grosshans, F.; Grangier, P. Continuous Variable Quantum Cryptography Using Coherent States, **Phys. Rev. Lett.** v.88, n.5, Feb 2002.

[38] Namiki, R.; Hirano, T. Security of quantum cryptography using balanced homodyne detection. **Physical Review A**, v.67, 022308, Feb 2003.

[39] Horak, P. The Role Of Squeezing In Quantum Key Distribution Based On Homodyne Detection And Post-Selection. **Journal Of Modern Optics**, v.51, n.8, p.1249-1264, May 2004.

[40] Wu, J.W. Violation of Bell's inequalities and two-mode quantum-optical state measurement. **Physical Review A**, v.61, 022111, Jan 2000.

[41] Ou, Z.Y.; Hong, C.K.; Mandel, L. Relation Between Input And Output States For A Beam Splitter. **Optics Communications**, v.63, n.2, p.118-122, Jul 1987.

[42] Miller, A.R. **The Cryptographic Mathematics of Enigma**. NSA, 2001. - Disponível em <http://www.nsa.gov/about/_files/cryptologic_heritage/publications/wwii/engima_cryptographic_

[43] **Wikipedia** - A Enciclopédia Livre / The Free Encyclopedia.
Artigos usados:
Cryptography, Criptografia, Cryptanalysis, Esteganografia, Charles Babbage, Alfabeto inglês, Difference engine, Gilbert Vernam, One-time pad, Hardware random number generator, Aritmética modular, Matemática modular, Enigma machine, Enigma (máquina), Cryptanalysis of the Enigma, Ultra, Bletchley Park, Alan Turing, Bombe, Colossus computer, Manchester Mark 1, ENIAC, Kerckhoffs's Principle, Criptografia de chave pública, Diffie-Hellman, RSA,

One-way function, Algoritmo de chave simétrica, Data Encryption Standard, AES, Brute-force attack, Digital signature, Assinatura Digital, Criptografia de curvas elípticas, Discrete logarithm, Hash, Universal hashing, MD5, RC5, RC6, SHA-1, PGP, Wigner quasi-probability distribution, Claude Shannon, Binary code, Quantum cryptography, Quantum key distribution, Quantum cryptography protocol, Secure Communication based on Quantum Cryptography, List of quantum cryptography protocols, Quantum communication channel, Fibre optic cable, Binary Search, Parity (telecommunication), Man-in-the-middle attack, Trojan horse, Denial of service attack, Kish cypher, No cloning theorem, Gilles Brassard, Charles H. Bennett (computer scientist).
Disponível em: <http://wikipedia.org/>

Observação Final e Indicaçao de Sites, Multimídias e Outros

As figuras utilizadas neste texto não confeccionadas pelo autor estão referenciadas e estão sob a Licença Creative Commons.

Como curiosidades e complementos aos tópicos abordados neste trabalho indicamos alguns sites onde é possível encontrar vídeos, palestras e materiais interativos relacionados à criptografia quântica:

[**A**] **Bletchley's code-cracking Colossus** - BBC News: Entrevistas e textos.
Disponível em <http://news.bbc.co.uk/2/hi/technology/8492762.stm>

[**B**] Seminários sobre **"Quantum Information, Computation and Complexity"** realizados no Institut Henri Poincaré (IHP).
Brassard, G. - Quantum cryptography (vídeo)
Ekert, A.K. - Introduction to quantum cryptography (video)
Bennett, C.H. - Quantum information and communication (video)
Disponíveis no site (aba *Lectures*) <http://www.quantware.ups-tlse.fr/IHP2006/>

[**C**] Bennett, C.H. General talk on Quantum Information 2006: **Information Is Quantum**.
Disponível em <http://www.research.ibm.com/people/b/bennetc/>

[**D**] Site com uma **Simulação Realística de uma Transmissão com o Protocolo BB84**:
<http://www.didaktik.physik.uni-erlangen.de/quantumlab/english/index.html>

[**E**] Duarte, O.C.M.B.; Fonseca, T.C.; Vaz, V.T. **Apresentação sobre Assinatura Digital** da disciplina de Redes de Computadores da UFRJ:
Disponível em <http://www.gta.ufrj.br/grad/07_1/ass-dig/index.html>

[**G**] Tkotz, V. - **Curso de Criptologia** do site "Aldeia Numaboa":
Disponível em <http://www.numaboa.com/criptografia>

[**H**] Goya, R.R. - **Curso de Introdução, História e Teoria da Criptografia**:
Disponível em <http://rgoya.sites.uol.com.br/criptografia/index.html>

[**I**] **Charles Babbage and his Difference Engine #2** (Youtube Video)
Disponível em <http://www.youtube.com/watch?v=KBuJqUfO4-w&NR=1>