Rafael Freitas Barbosa

Comunicações ópticas de espaço livre por contagem de fótons para uso em enlaces entre embarcações e estações costeiras

DISSERTAÇÃO DE MESTRADO

DEPARTAMENTO DE ENGENHARIA ELÉTRICA
Programa de Pós-graduação em Engenharia Elétrica

Rio de Janeiro
Março 2020

PONTIFÍCIA UNIVERSIDADE CATÓLICA
DO RIO DE JANEIRO

Rafael Freitas Barbosa

Comunicações ópticas de espaço livre por contagem de fótons para uso em enlaces entre embarcações e estações costeiras

Dissertação de Mestrado

Dissertação apresentada como requisito parcial para obtenção do grau de Mestre pelo Programa de Pós–graduação em Engenharia Elétrica do Departamento de Engenharia Elétrica da PUC-Rio.

Orientador: Prof. Guilherme Penello Temporão

Rio de Janeiro
Março de 2020

PONTIFÍCIA UNIVERSIDADE CATÓLICA
DO RIO DE JANEIRO

Rafael Freitas Barbosa

Comunicações ópticas de espaço livre por contagem de fótons para uso em enlaces entre embarcações e estações costeiras

Dissertação apresentada como requisito parcial para obtenção do grau de Mestre pelo Programa de Pós–graduação em Engenharia Elétrica da PUC-Rio. Aprovada pela Comissão Examinadora abaixo.

Prof. Guilherme Penello Temporão
Orientador
Centro de Estudos em Telecomunicações – PUC-Rio

Prof. Thiago Barbosa dos Santos Guerreiro
Departamento de Física – PUC-Rio

Dr. Giancarlo Vilela de Faria
Ouro Negro S.A. – Sistemas Laser

Rio de Janeiro, 06 de Março de 2020

Rafael Freitas Barbosa

Rafael Freitas Barbosa é graduado em Engenharia Elétrica com ênfase em eletrônica pela Pontifícia Universidade Católica do Rio de Janeiro (Rio de Janeiro, Brasil). É membro dos laboratórios de Fotônica e Optoeletrônica do Centro de Estudos em Telecomunicações da PUC-Rio e Capitão-de-Corveta do Corpo de Engenheiros da Marinha do Brasil.

Ficha Catalográfica

Barbosa, Rafael Freitas

Comunicações ópticas de espaço livre por contagem de fótons para uso em enlaces entre embarcações e estações costeiras / Rafael Freitas Barbosa; orientador: Guilherme Penello Temporão. – 2020.

161 f.: il. color. ; 30 cm

Dissertação (mestrado) - Pontifícia Universidade Católica do Rio de Janeiro, Departamento de Engenharia Elétrica, 2020.

Inclui bibliografia

1. Engenharia Elétrica – Teses. 2. Sistemas Híbridos Fibra-Óptica – Espaço-Livre;. 3. Comunicação Óptica em Espaço-Livre;. 4. Distribuição Quântica de Chaves;. 5. Criptografia Quântica;. 6. Comunicação no Infravermelho.. I. Temporão, Guilherme Penello. II. Pontifícia Universidade Católica do Rio de Janeiro. Departamento de Engenharia Elétrica. III. Título.

CDD: 621.3

Agradecimentos

Ao professor Guilherme Temporão, pela orientação e ideias ao longo de todo o curso, especialmente durante o desenvolvimento das configurações experimentais.

À minha esposa Thalitta e aos meus filhos Rafael e Alice, que abdicaram de parte de seu tempo comigo, sem deixar de lado o companheirismo, para tornar possível esta dissertação.

Aos modelos e exemplos morais e éticos que segui ao longo da vida nas pessoas de meu avô José†, meu pai Alberico†, meus tios Fernando e José Marcos e meu padrinho Pepe. À minha mãe, Maria José†, por ter me cobrado o estudo desde a primeira infância e ter me fornecido a educação que me trouxe até aqui.

Aos companheiros de laboratório, Pedro Tovar, Felipe Calliari, Matheus Esteves, Marlon Correa e Johnes Ricardo, sem os quais não teria sido possível a realização experimental deste trabalho, bem como ao Claiton Colvero, por ter desenvolvido os canhões transceptores e me auxiliado, mesmo de longe, a restaurá-los à operacionalidade. Também ao professor Jean Pierre, cujos incalculáveis conhcimento e experiência estão sempre à disposição no laboratório.

À Marinha do Brasil, na figura da Diretoria de Sistemas de Armas da Marinha, pela indicação e oportunidade de realizar este curso, e aos colegas de farda, em especial o CMG(EN) Miranda, o CC(EN) Póvoa e o CC(EN) Matheus. Ao amigo e instrutor Brian O'Brien† pelos ensinamentos profissionais e pessoais ao longo de nosso breve, mas intenso convívio.

À amiga Tatiana Pereira, pela revisão de todo este texto, com a maior paciência e dedicação, apesar do exíguo tempo disponível, e a todos aqueles que, de alguma forma, contribuíram para a conclusão deste trabalho.

Resumo

Barbosa, Rafael Freitas; Temporão, Guilherme Penello (Orientador). **Comunicações ópticas de espaço livre por contagem de fótons para uso em enlaces entre embarcações e estações costeiras** . Rio de Janeiro, 2020. 161p. Dissertação de Mestrado – Departamento de Engenharia Elétrica, Pontifícia Universidade Católica do Rio de Janeiro.

Este trabalho apresenta o estudo de comunicação óptica quântica no infravermelho, utilizando um sistema híbrido fibra-óptica – espaço-livre, como prova de princípio para o estabelecimento de chaves secretas a fim de utilização em criptografia do tipo *one-time pad*. Ao modular a polarização da luz de um laser em polarizações ortogonais, podem-se codificar os bits clássicos "1" e "0" em cada uma dessas polarizações, sendo detectadas por detectores contadores de fótons únicos, e, assim, utilizar o canal quântico para transmissão dos bits quânticos entre dois interlocutores, utilizando-os para o estabelecimento da chave criptográfica, que pode ser usada em qualquer tipo de informação a ser transmitida por um canal clássico ou quântico.

Ao realizar a transmissão em espaço-livre, sujeita a variações climáticas, como temperatura atmosférica, luz solar, presença de nuvens, chuva e vento, foi também estudada a influência destes fenômenos na qualidade da transmissão e dos dados obtidos.

Os resultados experimentais demonstraram consistência com a teoria e com outros trabalhos publicados na área até esta data com relação às taxas de erro de bit quântico e também à taxa de transmissão de bits. As taxas de erro obtidas, por estarem abaixo do limiar teórico para segurança da informação em comunicação quântica, provam, ainda, a possibilidade de estabelecimento de chave secreta para criptografia através do uso de distribuição quântica das chaves (QKD). Os resultados também apresentaram boa qualidade da informação recuperada após a descriptografia.

Palavras-chave

Sistemas Híbridos Fibra-Óptica – Espaço-Livre; Comunicação Óptica em Espaço-Livre; Distribuição Quântica de Chaves; Criptografia Quântica; Comunicação no Infravermelho.

Abstract

Barbosa, Rafael Freitas; Temporão, Guilherme Penello (Advisor). **Free-space photon counting optical communications for use in vessel-to-shore links**. Rio de Janeiro, 2020. 161p. Dissertação de Mestrado – Departamento de Engenharia Elétrica, Pontifícia Universidade Católica do Rio de Janeiro.

This work presents the study of optical quantum communication in the infrared region, using a hybrid optical-fiber – free-space system, as proof of principle for the agreement on secret keys by two parties for use in *one-time pad* encryption. By modulating the polarization of laser light into orthogonal polarizations, one can encode the classic bits "1" and "0" in each of these polarizations, being detected by single photon counter detectors, and can use the quantum channel to transmit the quantum bits between two interlocutors. It is then possible to use those bits to establish the cryptographic key, which can be used in any type of information to be transmitted by a classic or quantum channel.

While carrying out transmission in free space optics, subject to climatic variations, such as atmospheric temperature, sunlight, presence of clouds and rain, and the presence of wind, the influence of these phenomena on the quality of transmission and on the data obtained was also studied.

The experimental results showed consistency with the theory and with other works published to date with regard to quantum bit error rates and to the bit rate. The error rates obtained, being below the theoretical threshold for information security in quantum communication, further proves the possibility of establishing a secret key for encryption through the use of quantum key distribution (QKD). It also presented good quality on the information recovered after decryption.

Keywords

Hybrid Fiber-Optic – Free-Space Systems; Free-Space Optical Communication; Quantum Key Distribution; Quantum Cryptography; Infrared Communication.

Sumário

Lista de figuras

Lista de tabelas

Lista de Abreviaturas

AC – Corrente alternada
AFG – Gerador de Função Arbitrária (Arbitrary Function Generator)
AM – Modulação em Amplitude (Amplitude Modulation)
BATI – Boston Applied Technologies, Incorporated
BS – Divisor de Feixe (Beam Splitter)
CCD – Dispositivo de Carga Acoplada (Charge-Coupled Device)
CMOS – Semicondutor de Metal-Óxido Complementar
FLIR – Sistema de Infravermelho de Visão Frontal (Forward Looking Infrared)
FM – Modulação em Frequência (Frequency Modulation)
FPA – Matriz de Plano Focal (Focal Plane Array)
FPGA – Field Programmable Gate Array
FSO – Óptica de Espaço-Livre (Free-Space Optics)
FSOC – Comunicação Óptica em Espaço-Livre (Free-Space Optical Communication)
IR – Infravermelho (Infrared)
LWIR – Infravermelho de Longo Comprimento de Onda (Long-Wavelength Infrared)
MOSFET – Transistor de Efeito de Campo de Semicondutor de Metal-Óxido
OPM – Medidor de Potência Óptica (Optical Power Meter)
PBS – Divisor de Feixe Polarizador (Polarizing Beam Splitter)
PNS – Separação em Número de Fótons (Photon Number Splitting)
PC – Controlador de Polarização (Polarization Controller)
PM – Modulação em Fase (Phase Modulation)
QBER – Taxa de Erro de Qubit
QKD – Distribuição Quântica de Chaves (Quantum-Key Distribution)
SPAD – Detector de Fótons Únicos por Avalanche
SNR – Relação Sinal-Ruído (Signal-to-Noise Ratio)
VCSEL – Lasers de Emissão de Superfície de Cavidade Vertical (Vertical-Cavity Surface-Emitting Lasers)
VOA – Atenuador Óptico Variável (Variable Optical Attenuator)
WDM – Multiplexador por Divisão de Comprimento de Onda (Wavelength Division Multiplexer)

Sit down before fact with an open mind. Be prepared to give up every preconceived notion. Follow humbly wherever and to whatever abyss Nature leads or you learn nothing. Don't push out figures when facts are going in the opposite direction.

Admiral Hyman G. Rickover.

1
Introdução

Os sistemas de comunicação óptica diferem em princípio dos sistemas de microondas apenas na faixa de frequências da onda portadora utilizada para transportar a informação. As frequências das portadoras ópticas são tipicamente da ordem de 200 THz, em contraste com as frequências de portadoras de microondas, que são da ordem de 1 GHz. Um aumento na capacidade de informação de sistemas de comunicação óptica por um fator de até 10.000 é esperado simplesmente devido a essas altas frequências portadoras usadas para sistemas de ondas de luz [1]. Esse aumento pode ser entendido observando que a largura de banda modulada pode ser até alguns por cento da frequência da portadora. Tomando, por exemplo, 1% como o valor limite, sistemas de comunicações ópticas têm o potencial de transportar informação a taxas de até 2 Tb/s (em ordem de grandeza, pois, na realidade, o valor exato depende da modulação utilizada). É esse enorme potencial de largura de banda de sistemas de comunicação óptica que é a força motriz por trás do desenvolvimento e implantação mundial de sistemas de ondas de luz. Os sistemas atuais de ponta operam com taxas de bits da ordem de 10 Gb/s, indicando que há ainda considerável campo para aprimoramento.

A fibra óptica é o principal meio de propagação utilizado em aplicações ópticas na atualidade, interligando, hoje, várias partes do planeta. Entretanto, a utilização do espaço livre como meio de transmissão não foi deixada de lado e seu estudo não foi esquecido. Como um exemplo da aplicabilidade de comunicações ópticas em espaço livre, vemos a previsão de lançamento, ainda em março de 2020, e instalação em abril, do sistema europeu OSIRIS a bordo da nova plataforma Bartolomeo para a estação espacial internacional (ISS). O OSIRIS será capaz de estabelecer um link de comunicação em laser infravermelho direto para a Terra a uma taxa de até 10 $Gbps$ e a uma distância de até 1500 km [2].

Todavia, ainda que possível, é certo que os sistemas comerciais de comunicações ópticas não são e não serão todos completamente em espaço livre. Via de regra, há trechos em fibra óptica tanto no transmissor quanto no receptor, o que gera a necessidade do acpolamento da fibra óptica ao espaço livre e vice-versa.

Quando falamos de física quântica, então, a necessidade deste desenvolvimento fica ainda mais evidente. Empregando física quântica, vários objetivos que eram considerados impossíveis em um mundo clássico agora foram provados possíveis. Os links de comunicação quântica, por exemplo, são impossíveis de serem escutados sem detecção. Os computadores quânticos possibilitam a criação de novos algoritmos, que podem realizar de forma eficiente tarefas cujos algoritmos clássicos são extremamente ineficientes.

Um exemplo que ilustra o ponto e o impacto que os processadores quânticos de informação terão sobre todos nós é a segurança de muitas formas de criptografia, que são baseadas na dificuldade de fatoração de números suficientemente grandes. Encontrar os fatores de um número de 1024 dígitos levaria mais tempo do que a idade do universo em um computador projetado de acordo com as leis da física clássica e, ainda assim, pode ser feito num piscar de olhos em um computador quântico, se ele tiver um *clock* com velocidade comparável ao do computador clássico. O desafio é construir um destes!

Em realidade, talvez nem seja preciso que o computador quântico venha para quebrar este tipo de criptografia. Recentemente, um grupo da Tokyo University of Science produziu um chip capaz de resolver o *problema do caixeiro viajante* para até 22 cidades praticamente instantaneamente, o que levaria mais de 1200 anos em um computador padrão de alto desempenho [3]. E este chip usa algoritmo clássico! Nada impede que seja conseguido, num futuro próximo, um chip que resolva o problema da fatoração de números grandes em um tempo razoável, também utilizando um algoritmo clássico. Se isto ocorrer, a criptografia bancária, entre outras, estará condenada. Por mais que se busquem outras forma de criptografia que ainda não tenham sido quebradas, será uma *briga de gato e rato* entre as novas criptografias clássicas e as formas de quebrá-las. A criptografia quântica pode resolver este problema, uma vez que a segurança da informação é garantida pelas leis da física e não pela dificuldade ou demora de processar determinada informação. Desta forma, quanto antes for desenvolvida esta tecnologia, mais seguros nossos dados estarão.

Adicionalmente, a física quântica nos permitirá construir uma série de novas tecnologias não-clássicas, algumas exigindo recursos já realizáveis. Conforme divulgado pelo Financial Times [4], um artigo dos pesquisadores do Google, que foi publicado brevemente em um site da Nasa antes de ser removido, afirmou que seu processador era capaz de realizar um cálculo em três minutos e vinte segundos que levaria aproximadamente 10.000 anos no computador clássico mais avançado de hoje, conhecido como *Summit*. O computador quântico, chamado *Sycamore*, possui 53 bits quânticos e sucedeu um de 72 bits quânticos que era extremamente difícil de ser controlado. Quando

efetivamente funcionais, assim como os clássicos, os computadores quânticos em algum momento serão interligados por redes de computadores. Certamente estas redes de fibras ópticas também apresentarão trechos em espaço livre.

1.1 Radiação Infravermelha

A região infravermelha (IR) da radiação eletromagnética consiste daquela porção do espectro localizada entre os comprimentos de onda longos do espectro visível e os comprimentos de onda curtos de microondas. A banda espectral do IR é muitas vezes mais larga que o espectro óptico visível, que tem comprimentos de onda em torno de 0,30 μm até 0,72 μm. A banda de IR é, então, dividida em cinco regiões:

- IR próximo, entre 0,72 μm - 1,40 μm;
- IR de curto comprimento de onda, entre 1,4 μm - 3,0 μm;
- IR de médio comprimento de onda, entre 3,0 μm - 8,0 μm;
- IR de longo comprimento de onda (LWIR), entre 8,0 μm - 15,0 μm;
- IR distante, entre 15,0 μm - 1000 μm.

A real descoberta da radiação infravermelha foi resultado dos experimentos pioneiros de Sir William Herschel em 1800 [5]. Ao investigar a distribuição de energia térmica da radiação solar, Sir Herschel descobriu que a energia térmica aumentava em direção ao vermelho, dentro do espectro de luz visível, e continuava além da região visível. A conclusão óbvia foi de que a energia radiante existe além da região visível e a essa energia ele chamou "radiação invisível". Experimentos posteriores de Sir Herschel mostraram que essa "radiação invisível" obedece às mesmas leis que a luz visível.

Detectores de infravermelho são, em geral, usados para detectar, imagear e medir padrões da radiação térmica que todos os objetos emitem. A radiação infravermelha tem várias aplicações práticas muito importantes, como aquecimento de ambientes, cozimento de alimentos, secagem de tintas e vernizes, bem como amplo uso terapêutico para tratamento de sinusite, dores reumáticas e traumáticas. Outros exemplos práticos são os sistemas de alarme infravermelho, nos quais qualquer interrupção do feixe ocasiona a criação de um impulso elétrico no detector de controle, ligando o alarme, e também o impedimento de fechamento das portas de elevadores, evitando que elas se fechem sobre as pessoas. Mais um uso muito comum do infravermelho é para comandos a distância (controles remotos de aparelhos domésticos), preferíveis em relação às ondas de rádio porque não sofrem interferências de outras ondas eletromagnéticas

como, por exemplo, os sinais de televisão. A fotografia é também uma das atividades mais beneficiadas com a aplicação da radiação infravermelha. Algumas emulsões fotográficas podem se tornar sensíveis à luz de comprimento de onda de até 1, 1 *μm* – IR próximo, bem como é possível realizar detecção digital de imagens de radiação infravermelha com a utilização de dispositivos de carga acoplada (CCD), que é um sensor semicondutor. As imagens infravermelhas são utilizadas, entre outras aplicações, para sensoriamento remoto, identificação de queimadas e desmatamentos e, no campo militar, visão noturna e identificação de alvos em situações de baixa visibilidade. Ainda no campo militar, o infravermelho é utilizado em sistemas de controle de mísseis, controle de tiro e detecção de mísseis. Nas telecomunicações, o infravermelho é muito utilizado para transmissão através de fibras ópticas e também transmissão em espaço livre.

Das aplicações acima, comunicação em espaço livre é a aplicação desenvolvida neste trabalho. As instalações de fibras ópticas permitem o tráfego de dados em médias distâncias com altas taxas de transmissão e confiabilidade em grandes complexos industriais ou comerciais, mas, em muitos casos, a instalação de cabos ópticos torna-se inviável devido à complexidade e transtornos causados pelas obras de instalação ou inexistência de uma rota para passagem dos cabos. Este último é o caso da comunicação de um navio para outro navio de um comboio ou de navio para estação em terra. Uma solução que se apresenta viável para estes casos é a utilização da transmissão de sinais ópticos sem conexão física entre as extremidades do enlace. Este tipo de comunicação utiliza uma faixa do espectro óptico para a transmissão das informações pela atmosfera, formando um sistema de comunicações ópticas no espaço livre (FSOC).

Os sistemas de comunicação sem conexão física hoje existentes em navios são eficazes para se transmitirem dados entre eles. Entretanto, as informações transmitidas através destes sistemas estão sujeitas a interceptações por elementos adversos, que podem conseguir algum tipo de vantagem com as informações obtidas. Já os sistemas de FSOC, por serem sistemas direcionais, permitem uma comunicação segura entre transmissor e receptor, sem possibilidade de interceptação, se bem ajustados. A impossibilidade de detecção por elementos adversos permite, ainda, que sejam utilizados para troca e estabelecimento de chaves criptográficas secretas, que poderão ser utilizadas posteriormente para a transmissão de mensagens criptografadas através de qualquer sistema de comunicações, inclusive o FSOC.

Existem também algumas dificuldades associadas aos sistemas FSOC. O meio físico de transmissão é a atmosfera, logo, a transmissão está sujeita

a perturbações e oscilações que alteram de forma aleatória suas características, principalmente devido aos efeitos climáticos, como chuvas e nevoeiros, causando não só espalhamentos e absorção da luz, como também efeitos de cintilação. Para o caso dos navios, além dos efeitos mencionados, existe também o efeito dos canais de evaporação da água do mar e da presença de névoa devido à agitação mecânica da água (ondas), a depender das condições climáticas. Todos estes efeitos podem se apresentar associados no enlace, degradando em muito o sinal e dificultando a análise de cada um deles em separado. Há ainda a necessidade de existência de uma linha de visada livre entre o transmissor e o receptor e o alinhamento entre eles durante todo o tempo de transmissão, o que pode ser de difícil obtenção em comunicações envolvendo embarcações, devido ao balanço.

1.2 Breve História da Criptografia Quântica

A criptografia quântica permite que dois usuários se comuniquem com perfeita segurança da informação (comprovadamente), mesmo que eles não tenham estabelecido previamente uma chave secreta longa, ainda que haja um espião escutando o canal durante a transmissão. A segurança da informação é mantida mesmo se o espião tiver acesso a poder computacional ilimitado e cuja tecnologia é limitada somente pelas leis fundamentais da física [6].

A criptografia quântica teve sua origem em 1982, com a publicação do *paper* de Bennett, Brassard, Breidbart e Wiesner [7], no qual o termo foi usado pela primeira vez. A primeira ideia para a criptografia quântica surgiu de uma conversa entre Bennett e Brassard, ocorrida três anos antes, na qual Bennett expôs a ideia de seu amigo Wiesner (em torno de dez anos antes) do uso da física quântica para evitar falsificação de cédulas monetárias. Ambas as ideias se baseiam no princípio da não-clonagem, um princípio fundamental da física quântica, que garante que é impossível realizar uma cópia exata de um estado quântico desconhecido, o que torna impossível realizar escuta no canal quântico sem ser detectado.

Mas a ideia de usar o canal quântico para transmitir uma chave secreta aleatória arbitrariamente comprida, em vez de transmitir a informação criptografada em si, só lhes ocorreu um ano depois. Se a escuta fosse detectada no canal quântico, devido a distúrbios inevitáveis causados pela escuta, a chave seria jogada fora; caso contrário, poderia ser usada com segurança para transmitir uma mensagem sensível pelo uso do esquema clássico de *one-time pad*. Em essência, esse desvio através do *one-time pad* permitiu mudar o canal de *detecção* de escuta fornecido pela natureza em um canal de *prevenção* de es-

cuta [6]. Outra vantagem do uso do canal quântico para distribuição de chaves em vez de transmissão de informação é que ele é mais robusto quanto à perda de fótons, uma vez que uma subsequência aleatória de bits de uma sequência aleatória de bits é ainda uma sequência aleatória de bits, ainda que mais curta. Assim surgiu a Distribuição de Chaves Quânticas (QKD).

O protocolo BB84 para QKD, que é usado até os dias de hoje e foi inspiração para vários outros protocolos que dele derivaram, foi primeiro apresentado oralmente no simpósio *IEEE Symposium on Information Theory* de 1983 e publicado pela primeira vez em dezembro de 1984 [8]. Leva em seu nome as iniciais de seus proponentes, Bennett e Brassard, e o ano de sua publicação. Em 1989, os criadores do BB84 concluíram a construção de um protótipo e realizaram a primeira transmissão de chave quântica secreta, utilizando o protocolo, a uma distância de 32, 5 *cm*. Este foi o ponto de partida para finalmente atrair o interesse da comunidade científica.

Em 1991, Artur Ekert reinventou o QKD [9], incluindo o emaranhamento quântico de fótons e a violação da desigualdade de Bell no protocolo BB84, uma ideia que gerou muitos frutos, principalmente após a invenção da destilação do emaranhamento e da amplificação de privacidade. O E91, como foi chamado o novo protocolo proposto por Ekert, tornou mais simples a prova da segurança incondicional do BB84 original, que não tinha emaranhamento.

A produção científica atual e o desenvolvimento de aplicações em informação quântica são tão grandes, que foi surgindo, paulatinamente, uma necessidade de adaptação do mercado de telecomunicações à nova realidade. A criptografia quântica, por exemplo, já foi utilizada em algumas aplicações práticas, inclusive transferência bancária e transmissão entre duas cidades de resultados de eleição, e já pode ser encontrada comercialmente disponível. Hoje há quatro empresas que oferecem sistemas de QKD e várias grandes empresas possuem programas de pesquisa que incluem a criptografia quântica.

1.3 Organização desta Dissertação

Neste trabalho, apresentamos um estudo do espaço livre como meio de propagação para comunicações ópticas no infravermelho próximo (janela atmosférica de 1550 *nm*), por contagem de fótons, como prova de princípios para o estabelecimento de chaves criptográficas via QKD e a avaliação da aplicabilidade desta forma de comunicação para embarcações. O trabalho, realizado experimentalmente, consistiu de um sistema híbrido fibra óptica – espaço livre para a realização do enlace e apresentou três fases distintas.

A primeira fase consistiu de um aprofundamento do estudo teórico e da

recuperação da operabilidade de equipamentos ópticos antigos essenciais ao desenvolvimento experimental, bem como do teste e escolha da configuração experimental mais adequada aos nossos objetivos, inclusive quanto à forma de codificação dos *bits quânticos* (qubits).

Na segunda fase, foi realizada a parte experimental em laboratório, com o objetivo de caracterizar os equipamentos individualmente e em conjunto, formando o sistema. Nesta fase foram estabelecidas chaves criptográficas conciliadas, com a medição dos parâmetros da comunicação, para análise.

A terceira fase envolveu a instalação do sistema nos telhados de dois edifícios situados dentro do campus da PUC-Rio a 160 *m* de distância, sujeitos a todas as intempéries, e o estabelecimento de comunicações utilizando o mesmo sistema da fase anterior. Nesta fase também foram estabelecidas chaves criptográficas conciliadas, com a medição dos parâmetros da comunicação, para comparação com os resultados obtidos em laboratório e análise dos efeitos do canal atmosférico no resultado obtido.

Esta dissertação está organizada da seguinte forma: o capítulo 2 apresenta os conceitos fundamentais das comunicações ópticas em espaço livre; no capítulo 3, os conceitos das comunicações quânticas; o capítulo 4 concentra-se em descrever o processo de desenvolvimento e teste das configurações experimentais, bem como descrever brevemente as características e a função de cada equipamento dentro da configuração; no capítulo 5 são descritos os procedimentos de alinhamento e calibração do sistema, o procedimento de análise dos dados obtidos e são apresentados e discutidos os resultados experimentais realizados tanto em bancada, em configuração back-to-back, quanto ao ar livre, nos telhados dos edifícios e, finalmente, uma conclusão do trabalho realizado é fornecida no capítulo 6.

1.4
Visão Histórica – Radiação Infravermelha

A tecnologia de infravermelho existente hoje é resultado de várias descobertas e desenvolvimentos de muitos cientistas ao longo dos últimos duzentos anos. Listadas abaixo, em ordem cronológica, estão as principais conquistas que tiveram influência na elaboração deste trabalho.

Marcos do estudo da radiação infravermelha ([5], [10])

– 1800: Sir William Herschel, com o uso de termômetros e um prisma, descobre que a energia térmica aumenta em direção ao vermelho, dentro do espectro de luz visível, e continua além da região visível. Descobre, ainda, que a radiação IR obedece às mesmas leis que a luz visível.

– 1821: T.J. Seebeck descobre o efeito termoelétrico usando um par de cobre e antimônio.

– 1830: L. Nobili desenvolveu o termopar, que detecta radiação infravermelha com maior grau de sensibilidade que os termômetros.

– 1833: L. Nobili e M. Melloni desenvolvem a termopilha, um sensor ainda mais preciso que o termpopar. A termopilha consiste na integração de vários termopares. O desenvolvimento destes dois dispositivos é considerado o primeiro passo importante no avanço da tecnologia do infravermelho.

– 1840:Sir John Herschel, filho de Sir William Herschel, descobre as três janelas atmosféricas.

– 1843: E. Becquerel descobre os efeitos fotográfico e fosforescente da radiação infravermelha.

– 1847: Fizeau, Foucault e Knoblauch ilustram que a radiação IR exibe efeitos de interferência de maneira exatamente igual à luz visível. Esta prova colocou fim à controvérsia de que a radiação IR e a luz visível são similares em vários aspectos básicos.

– 1864: J.C. Maxwell publica a teoria da radiação eletromagnética.

– 1873: Willoughby Smith descobre os princípios de fotocondutividade usando selênio.

– 1876: W.G. Adams and A.E. Day descobrem o efeito fotovoltáico no selênio.

– 1879: J. Stefan descobre a relação empírica entre a intensidade da radiação e a temperatura de um corpo negro.

– 1880: S. P. Langley inventa o primeiro bolômetro, baseado na variação da resistência ôhmica com o calor gerado pela radiação incidente, e que é consideravelmente mais sensível que a termopilha.

– 1883: M. Melloni realiza estudos das características de transmissão de materiais transparentes ao IR.

– 1890: J. Elster and H. Geitel constróem um detector fotoemissivo consistindo de um catodo de metal alcalino.

– 1894,1900: J.W. Rayleigh and W. Wien derivam a relação de comprimento de onda da radiação de corpo negro.

– 1900: Max Planck descobre as propriedades quânticas da luz.

– 1903:W.W. Coblentz realiza a medição de temperatura de estrelas e planetas usando radiometria infravermelha e espectrometria.

– 1904: Bose descobre as propriedades fotosensitivas do sulfeto de chumbo (PbS).

– 1905 Albert Einstein estabelece a teoria da fotoeletricidade.

– 1914: Aplicação de bolômetros para exploração remota de pessoas (200 *m*) e aeronaves (1000 *m*).

– 1917 - 1920: T. W. Case reporta as propriedades fotocondutoras do PbS e desenvolve um detector fotocondutor que é mais sensível e com resposta mais rápida que os termopares e os bolômetros. Este foi o primeiro detector fotocondutor para uso em sistemas de transmissão e recepção em IR, o que estimulou um grande interesse em IR.

– 1928: G. Holst, J.H. de Boer, M.C. Teves e C.F. Veenemans propõem a ideia do conversor eletroóptico (incluindo o de multiestágio).

– 1929: L.R. Kohler desenvolveu um tubo conversor com um fotocatodo (Ag/O/Cs), sensível ao infravermelho próximo.

– 1930: Gudden, Görlich e Kutscher desenvolvem localizadores de direção em infravermelho baseados em detectores quânticos de PbS no comprimento de onda de 1, 5 *μma*3, 0 *μm* para aplicações militares, com alcance extendido durante a Segunda Guerra Mundial para 30 *km* para navios e 7 *km* para tanques (3 *a*5 *μm*)

– 1934: Primeiro conversor de imagem IR.

– 1939: Desenvolvimento da primeira unidade de *display* IR nos EUA (*sniperscope, snooperscope*)

– 1941: R.S. Ohl observa o efeito fotovoltáico de uma junção p-n de silício.

– 1942: G. Eastman (Kodak) apresentou o primeiro filme sensível ao infravermelho.

– 1947:M.J.E. Golay desenvolveu o detector de alta-detectividade de radiação, com ação pneumática.

– 1954: Primeiras câmeras de imagens baseadas em termopilhas (tempo de exposição de vinte minutos por imagem) e em bolômetros (quatro minutos).

– final de 1940's - início de 1950's: Cashman, McFee e Levinstein expandiram a tecnologia do PbS para detectores a seleneto de chumbo (PbSe)telureto de chumbo (PbTe) e antinometo de índio (InSb).

– final dos anos 1940: Burstein desenvolve os primeiros detectores a fotocondutores extrínsecos, de germânio dopado com ouro, germânio dopado com zinco e germânio dopado com cobre. A maioria destes detectores necessitava de refrigeração a temperaturas variando de 4K a 40K.

– 1955: Início da produção em massa de cabeças guiadas a IR para mísseis nos EUA (detectores de PbS and PbTe e, posteriormente, de InSb para mísseis Sidewinder).

– 1957: W.D. Lawson, S. Nelson e A.S. Young desenvolvem a liga de HgCdTe como material detector de IR. Este detector requeria refrigeração a apenas 77K (nitrogênio líquido).

– 1961:Descoberta do germânio dopado com mercúrio e sua aplicação (*linear array*) nos primeiros sistemas LWIR FLIR.

– 1965:Inícioda produção em massa de câmeras IR para aplicações civis na Suécia (AGA Thermografiesystem 660).

– 1970: W.S. Boyle e G.E. Smith desenvolvem o dispositivo de carga acoplada (CCD).

– 1970: Início da produção de sensores de IR em matriz (Matriz monolítica de Si: R.A. Soref 1968; IR-CCD 1970; matriz de diodos Schottky: F.D. Shepherd e A.C. Yang 1973; IR-CMOS 1980; SPRITE: T. Elliot 1981).

– 1975: Lançamento de programas nacionais para desenvolvimento de sistemas de observação de alta resolução espacial no infravermelho com detectores multielementos integrados em um mini-refrigerador (chamados de sistemas de primeira geração): Módulo comum – CM (EUA), módulo comum de imagem térmica – TICM (UK) e sistema térmico modular – SMT (França).

– 1975: Primeira matriz de plano focal (FPA) híbrida de Índio.

– 1977: G.A. Saihalasz, R. Tsu, and L. Esaki desenvolvem as superestruturas de tipo II de InAs/GaSb.

– 1980: Desenvolvimento e produção de sistemas de segunda geração (câmeras de FPA híbridos).

– 1985: Desenvolvimento e produção em massa de câmeras com FPA de diodo Schottky (siliceto de platina).

– 1990: Desenvolvimento e produção do sistema híbrido de segunda geração poço quântico fotocondutor de infravermelho.

– 1995: Início da produção de câmeras IR com FPA não refrigerados, baseados em microbolômetros e piroelétricos).

– 2000: Desenvolvimento e produção de sistemas de IR de terceira geração.

– 2005: Início do aprofundamento do estudo de comunicações ópticas submarinas sem fio.

– 2014: O sistema OPALS (Optical PAyload for Lasercomm Science) da NASA foi enviado à Estação Espacial Internacional (ISS), com o objetivo de testar o potencial do uso de um laser infravermelho para transmitir dados do espaço para a Terra ([11],[12]).

– 2020: Previsão de lançamento em março de 2020, e instalação em abril, do sistema europeu OSIRIS a bordo da nova plataforma Bartolomeo para a ISS. O OSIRIS será capaz de estabelecer um link de comunicação em laser infravermelho direto para a Terra a uma taxa de até 10 *Gbps* e a uma distância de até 1500 *km* [2].

1.5 Visão histórica – Criptografia Quântica

A criptografia quântica é uma área de estudos muito recente ainda no mundo científico e oferece infinitas possibilidades de avanço em um futuro próximo, principalmente após a criação dos computadores quânticos. Listados abaixo estão os principais marcos do desenvolvimento da criptografia quântica.

Marcos do desenvolvimento da criptografia quântica

– fim dos anos 1960: S. Wiesner apresenta a C. Bennett suas ideias para o uso da física quântica para evitar falsificação de cédulas monetárias e para um canal de multiplexação quântica [6].

– 1979:C. Bennett apresenta as ideias de Wiesner a G. Brassard e eles iniciam as discussões sobre o tema [6].

– 1982: Publicação do primeiro *paper* sobre criptografia quântica, por Bennett, Brassard, Breidbart e Wiesner ([6], [7]).

– 1983: Surgimento da ideia de Bennett e Brassard para utilizar o canal quântico para QKD, ao invés de transmitir a informação propriamente dita [6].

– 1984: Bennett e Brassard criam o protocolo BB84, para distribuição de chaves quânticas secretas [8].

– 1989: Bennett e Brassard, com a ajuda de outros, realizam a primeira transmissão de chave quântica secreta em um protótipo com 32, 5 *cm* de distância de transmissão [6].

– 1991: A. Ekert cria o protocolo E91, que introduz o emaranhamento quântico de fótons e a violação da desigualdade de Bell no BB84 [9].

– 2003: Lançado o primeiro sistema comercial de QKD do mundo, pela empresa americana MagiQ Technologies, Inc [13].

– 2004: Primeira transferência bancária documentada no mundo a usar QKD foi realizada em Viena, Áustria [14].

– 2004 - 2007: Operação da DARPA Quantum Network, em Massachussetts, EUA, uma rede de QKD de dez nós que funcionou ininterruptamente durante seu tempo de operação. Foi basicamente uma rede padrão de computadores via internet, protegida por distribuição de chaves quânticas [15].

– 2007: Tecnologia de criptografia quântica foi usada na Suíça para transmitir resultado de eleições da cidade de Genebra para a capital do país, Berna [16].

– 2009 - 2011: A Swiss Quantum concluiu com êxito o projeto mais antigo para testar QKD em campo. O principal objetivo da rede Swiss Quantum, instalada na região metropolitana de Genebra em março de 2009, era validar a confiabilidade e a robustez do QKD em operação contínua em uma rede por um longo período em ambiente de campo [17].

– 2011: Início dos testes de campo da Tokyo QKD Network, uma rede de comunicações segura, baseada em QKD [18].

– 2013: O Batelle Memorial Institute instalou a primeira rede protegida por QKD dos EUA, ligando seu campus principal em Columbus, Ohio, a sua instalação industrial, situada próximo a Dublin, também em Ohio [19].

– 2016: A missão espacial QUESS, da China, lançou o primeiro satélite de pesquisa para comunicação quântica, o “Micius”, com o objetivo de criar um link entre Beijing e Viena, a uma distância terrestre de 7500 *km* ([20],[21]).

– 2017: Uma linha de fibra óptica terrestre de 2000 *km* ligando Beijing, Jinan, Hefei e Shanghai se tornou operacional. No mesmo dia, foi realizada uma chamada de video entre Beijing e Viena, usando o canal do satélite “Micius”. Juntos, eles constituem a primeira rede quântica espaço-Terra ([22],[23]).

– 2019: O Google afirma ter construído o primeiro computador quântico que pode realizar cálculos além da capacidade dos supercomputadores mais poderosos da atualidade [4].

2
Comunicações Ópticas em Espaço Livre

Qualquer sistema de comunicações ópticas pode ser simplificadamente esquematizado como na figura 2.1, apresentando um transmissor óptico, onde está incluída a fonte de luz, bem como a codificação da informação em sinal óptico; o canal óptico, no qual a informação trafegará, e o receptor óptico, cuja função é detectar o sinal transmitido e tratá-lo da forma adequada, que permita a restauração do sinal à informação original.

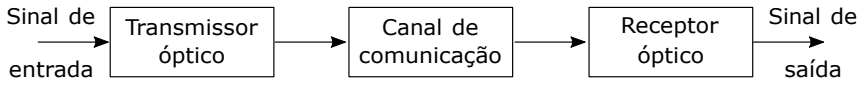


Figura 2.1: Esquema de um sistema genérico de comunicações ópticas.

Os primórdios da comunicação óptica datam de fevereiro de 1880, quando Alexander Graham Bell e seu assistente, Sumner Tainter, executaram a primeira demonstração conhecida da transmissão da fala através de um feixe de luz modulada, usando um aparelho que ele chamou de fotofone [24]. O transmissor do fotofone consistia de um bocal, em frente ao qual o locutor se postava, e um espelho, que vibrava de acordo com a pressão acústica transmitida pela voz do locutor. A vibração deste espelho modulava a intensidade de raios de luz incidentes sobre sua superfície. Bell utilizou um outro espelho para refletir raios de luz em direção a uma lente, que os direcionava ao espelho modulador. O dispositivo receptor, colocado a certa distância, concentrava a luz recebida sobre uma barra de selênio. As variações na luz fazem com que a resitência elétrica do selênio varie e, como consequência, a corrente elétrica passando pela barra varia. Em série com a barra de selênio, existia um circuito com um par de fones. A componente alternada da corrente gerava as ondas mecânicas de áudio ao fazer vibrar as placas metálicas nos fones segundo as formas de onda da fala que estava sendo transmitida.

Em realidade, a óptica já era usada para comunicar informações pelo espaço livre desde a antiguidade, mas de forma primitiva. *Aeschylus* relata o uso da óptica para a transmissão até Argos, da notícia da queda de Tróia para os gregos, em torno do ano 1.200 a.C [25]. A distância entre as duas cidades era de centenas de milhas e a informação foi recebida em Argos apenas algumas

horas depois da conquista. Quando da invasão da Espanha à Inglaterra em 1588, dentro de 30 horas desde que a Armada Espanhola foi avistada, mais de 70.000 homens já haviam sido convocados para a guerra, tendo sido a maioria deles dentro de 24 horas. Esta rapidez na comunicação só foi possível com a utilização de um sistema óptico em espaço livre [26]. Segundo F. Mims [24], W.D. Smithers descreve um sistema de comunicação usado no México que utiliza pequenos espelhos de bolso para transmitir longas mensagens complexas através da reflexão da luz solar. Ele ainda especula que este método foi utilizado pelos aztecas para avisar Montezuma minutos após a chegada de Cortez a Veracruz, a uma distância de quatro dias de viagem a cavalo. Somente aqueles versados na arte de *avisadores* são capazes de transmitir e decifrar as mensagens através deste antigo método azteca.

Os modos primitivos de comunicação óptica usados na Grécia antiga e na Inglaterra conforme descritos acima, conquanto efetivos, não continham exatamente uma informação transmitida, mas sim uma sinalização previamente acordada, como um bit, enquanto que o método azteca necessitava de um conhecimento prévio da codificação dos sinais. O fotofone foi o primeiro aparelho capaz de trazer a comunicação óptica em espaço livre portando efetivamente informação e com a possibilidade de ser transmitida e recebida por qualquer pessoa, ainda que leiga. Historicamente, a transmissão da voz humana via modulação da luz (fotofone) precedeu a transmissão da voz em ondas de rádio em pelo menos 15 anos.

Por volta da década de 1960 começaram a surgir os modernos sistemas de transmissões em FSO, a partir do aparecimento dos LEDs semicondutores. Com respeito à topologia dos enlaces, os sistemas de FSO atuais apresentam muita semelhança com os sistemas ópticos a fibra. A grande diferença é o meio de propagação. A fibra é um meio que confina a luz e, portanto, devem-se analisar os efeitos de atenuações, dispersões e alguns efeitos não-lineares, a depender da aplicação, com muito pouca influência externa na variação destes parâmetros com relação à informação transmitida. Já no espaço livre, o meio de propagação é a atmosfera, em que não nos preocupamos com dispersões comuns às fibras ópticas, mas, por outro lado, existem outros fatores decisivos para manter uma boa relação sinal-ruído (SNR), como, por exemplo, absorção, turbulências e espalhamentos da luz. Um agravante é que o meio não apresenta homogeneidade em todo o percurso do feixe luminoso e também depende de uma série de fatores e condições que variam muito rapidamente ao longo de um dia, indo desde condições ótimas de propagação até a indisponibilidade temporária do canal, com impossibilidade de estabelecimento de conexão. Já os demais dispositivos envolvidos numa transmissão em FSO são idênticos no

princípio de funcionamento aos dispositivos para transmissões em fibras: as fontes de luz (laser ou LED), os moduladores, demoduladores, protocolos de transmissão e correção de dados, os receptores e demais dispositivos utilizados nas transmissões ópticas de altas taxas.

As principais características básicas dos transmissores ópticos, do meio de transmissão e dos receptores ópticos serão discutidas, nesta sequência, ao longo deste capítulo.

2.1
Sistemas Transmissores

Em geral, os sistemas transmissores em FSO têm as mesmas características que seus equivalentes para transmissões em fibras, necessitando observar, apenas, algumas peculiaridades do sistema em espaço livre, como potência óptica adequada e comprimento de onda nas janelas de transmissão mais favoráveis da atmosfera. A função dos transmissores ópticos é converter um sinal elétrico de entrada no sinal óptico correspondente e lançá-lo no canal de comunicação. Desta forma, os sistemas de comunicação óptica mais simples são compostos de uma fonte de luz, um mecanismo de modular esta luz de alguma forma de acordo com a informação a ser transmitida e um equipamento para acoplar a luz modulada no meio de transmissão, seja ele qual for. A depender das características do sistema ou do meio, pode ser necessário também amplificar ou atenuar a potência óptica antes do acoplamento no meio.

2.1.1
Fontes Ópticas

Os materiais semicondutores cumprem muito bem a função de conversão de sinal elétrico em luz e, portanto, são muito utilizados como fontes ópticas em sistemas de comunicação. Uma fonte óptica de semicondutor é composta por uma junção p-n, formada ao se juntar um semicondutor tipo *p* em contato com um do tipo *n*. Um semicondutor do tipo *n* tem uma fonte adicional de elétrons livres na banda de condução e o material tipo *p* tem um número de buracos, ou lacunas, livres. O nível de Fermi (E_f), que em materiais semicondutores intrínsecos (não dopados) fica situado entre as bandas de condução e de valência, no meio da separação (*gap*) entre as bandas, é movido para dentro da banda de condução em semicondutores do tipo *n* fortemente dopados (E_{fc}). Da mesma forma, em semicondutores *p* fortemente dopados, o nível de Fermi é movido para dentro da banda de valência (E_{fv}). Quando um material tipo *n* e um material tipo *p* são colocados juntos, em equilíbrio térmico, há um processo de difusão de elétrons e buracos através da junção p-n e eles se

recombinam na região da interface, de modo a manter contínuo o nível de Fermi através da junção. Assim, durante este processo, forma-se um campo elétrico que funciona como uma barreira (região neutra) que elétrons e buracos não tem energia suficiente para atravessar, o que impede a continuação da difusão. Este é dito o campo elétrico intrínseco, ou interno, da junção p-n. Ao aplicarmos uma tensão elétrica externa direta nesta estrutura, a barreira diminui e o potencial de energia dos elétrons livres no material tipo *n* aumenta. Desta forma, os elétrons e as lacunas têm energia suficiente para atravessar a junção e a difusão é reiniciada. Como resultado desse movimento de portadores de carga, é observada uma corrente elétrica, que aumenta exponencialmente em função da tensão elétrica aplicada. Nessas condições, elétrons e buracos estão presentes simultaneamente na região de depleção (a região em torno da junção) e podem se recombinar de forma espontânea ou estimulada. Quando um elétron recombina com um buraco, este elétron tem uma queda para a camada de valência e, durante este processo, a energia excedente é liberada na forma de um fóton. O comprimento de onda (λ) da luz emitida durante este processo depende da energia E_g do *gap* entre as camadas do material. Ou seja, a partir da escolha do material utilizado, seleciona-se automaticamente o comprimento de onda da luz emitida. A equação (2-1) representa a relação entre eles, onde h é a constante de Planck e c a velocidde da luz.

$$\lambda \approx \frac{h.c}{E_g} \tag{2-1}$$

A figura 2.2 ilustra esquematicamente dois estados de um átomo: o estado fundamental, E_1, e o estado excitado, E_2, e os três processos atômicos fundamentais envolvendo a luz. Se a energia hv de um fóton de luz incidente de freqüência v for aproximadamente igual à diferença de energia entre os dois estados, $E_g = E_2 - E_1$, ocorre a absorção do fóton pelo átomo e ele vai para o estado excitado. Os átomos podem se excitar por absorção de diferentes fontes de energia: calor, luz, vibração, som, choques mecânicos, descargas elétricas ou radiações eletromagnéticas. Átomos excitados eventualmente retornam para seu estado fundamental e emitem luz neste processo. Se o retorno ao estado fundamental ocorre de forma natural, diz-se que há uma emissão espontânea de luz. Se ocorre iniciada por um fóton existente, diz-se emissão estimulada.

A emissão espontânea ocorre quando um elétron de um átomo excitado, no estado E_2, sofre uma transição para o estado fundamental, E_1, independentemente do número de fótons presentes no material, e emite um fóton de energia hv no processo. A probabilidade de uma emissão ocorrer num intervalo de tempo entre t e $t + \Delta t$ é dado por $p_{sp}\Delta t$, onde p_{sp} é a densidade de probabilidade (por segundo) dessa transição espontânea e depende da frequência

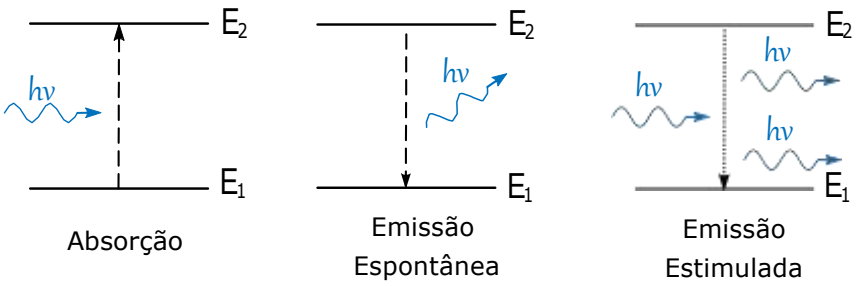


Figura 2.2: Processos atômicos fundamentais entre dois níveis de energia.

v [27]. Os fótons oriundos de emissões espontâneas são emitidos em instantes aleatórios, em direções aleatórias e com polarizações aleatórias, ou seja, cada um com sua direção de propagação, com sua polarização e com sua fase, sem correlação de fase entre si. Diz-se incoerente a luz com estas características.

A emissão estimulada ocorre quando, em um átomo no estado excitado, indice um fóton de energia hv, aproximadamente igual à energia do *gap* ($hv \approx E_g$) entre os níveis excitado e fundamental do átomo e este fóton induz no átomo a emissão de um outro fóton, juntamente com o decaimento do átomo do estado excitado para o estado fundamental. O fóton emitido é um "clone" do fóton incidente, apresentando a mesma frequência, direção de propagação, polarização e fase que aquele. Diz-se coerente a luz com essas características. Como os eventos de estimulação da emissão de fótons são mutuamente exclusivos entre si, para um mesmo volume de um mesmo material, a densidade de probabilidade de emissão estimulada de *um* fóton é diretamente e linearmente proporcional à quantidade de fótons incidentes no material [27].

Os LEDs são junções p-n de material semicondutor diretamente polarizado por uma tensão elétrica externa. Pelo processo já descrito anteriormente, de emissão espontânea, quando há recombinação de pares elétron-buraco na região de depleção, há simultaneamente emissão de fótons, não correlacionados entre si, o que dá origem à luz incoerente. Enquanto for mantida a tensão externa, a taxa de emissão de fótons se manterá. Parte desses fótons ($\approx 1,4\%$ da potência óptica interna) consegue escapar do material e pode ser, então, utilizada no sistema óptico desejado. Este cálculo não apresenta maiores dificuldades e pode ser encontrado na Seção 3.2.1 da referência [1].

Os lasers, por outro lado, emitem luz através do processo de emissão estimulada e, portanto, coerente. Em equilíbrio térmico na temperatura ambiente, o processo de emissão espontânea é dominante com relação à absorção e à emissão estimulada para radiação na região visível ou infravermelho próximo ($hv \sim 1\ eV$). Desta forma, os lasers devem operar fora do equilíbrio térmico,

para alterar a relação de dominância. A forma utilizada para isso é o bombeamento de energia por uma fonte externa. Ainda assim, a emissão estimulada concorre com o processo de absorção e pode não ser o evento dominante. Conseguirá ser o processo dominante somente se houver inversão de população, isto é, a densidade atômica no estado excitado E_2 deve ser maior que a densidade atômica no estado fundamental E_1, o que não é possível de acontecer em sistemas em equilíbrio térmico. Portanto, a inversão de população é pré-requisito para o funcionamento dos lasers e é atingida quando a densidade de portadores injetados na camada ativa excede um certo valor, conhecido como o valor de transparência. A partir deste ponto, a região ativa apresenta ganho óptico e um sinal óptico se propagando na região ativa seria amplificado proporcionalmente à exponencial do ganho. Além do ganho, é necessário que haja realimentação no sistema, convertendo o amplificador óptico em um oscilador óptico, que faça com que parte da luz gerada por amplificação retorne ao meio de ganho e seja amplificada novamente. Isto é conseguido colocando-se o meio de ganho entre dois espelhos (ou faces refletoras) com reflexividade menor que 100%, formando uma cavidade de Fabry-Perot. Se a distância percorrida em uma volta completa dentro da cavidade for tal que a fase se altera de um múltiplo de 2π, haverá ali interferência construtiva. Dentro da cavidade, os fótons são gerados em todas as direções e vários comprimentos de onda, mas apenas os que se propagam na direção dos espelhos são refletidos e voltam pela mesma cavidade gerando mais um fóton. Assim, a luz é amplificada apenas pelos fótons de mesma energia, direção e comprimento de onda. Uma parte deste feixe luminoso gerado dentro da cavidade ressonante para este comprimento de onda escapa para fora pela janela do espelho, e este será o feixe laser emitido. Finalmente, para que haja um feixe laser, é necessário que mais uma condição seja satisfeita: o ganho obtido deverá ser maior do que as perdas nos espelhos e perdas internas, que incluem absorção, espalhamento e outros mecanismos. A corrente elétrica necessária para induzir este ganho superior às perdas é conhecido como corrente limiar de laser. O ganho na cavidade é diferente para cada comprimento de onda , logo, é possível que o laser esteja emitindo em algum(uns) comprimento(s) de onda e, mesmo sendo um comprimento de onda possível na cavidade, determinado modo não esteja presente no feixe de laser emitido, pois seu ganho não supera as perdas, como pode ser visto no gráfico ilustrativo da figura 2.3.

Na prática, o sistema de dois níveis exemplificado na figura 2.2 não é realizável. Em sistemas atômicos, isso é alcançado usando esquemas de bombeamento de três e quatro níveis, de modo que uma fonte externa de energia aumente a população atômica do estado fundamental para um estado

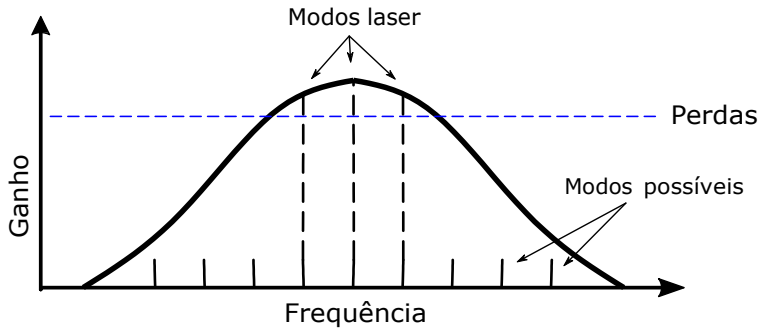


Figura 2.3: Perfis de ganho e perdas em lasers semicondutores. Somente os modos com ganho maior que as perdas fazem parte do feixe laser. Barras verticais mostram os locais dos modos longitudinais possíveis na cavidade.

excitado de energia acima da energia do estado E_2. Naturalmente esta é apenas uma explicação básica dos conceitos de funcionamento dos dispositivos lasers, amplamente desenvolvidos em diferentes bibliografias mais específicas sobre o assunto.

As fontes ópticas utilizadas em comunicações podem ser incoerentes, como os LEDs, ou coerentes, como os lasers, a depender da necessidade de potência e das taxas de transmissão, bem como dos custos com que se possa, ou queira, trabalhar. Em um LED, os fótons gerados são oriundos de emissões espontâneas, emitidos em instantes aleatórios e em direções aleatórias, ou seja, cada um com sua direção de propagação e com sua fase, sem correlação de fase entre si. Ademais da incoerência, os LEDs apresentam largura espectral relativamente grande (30 *a* 60 *nm*) e baixa potência de transmissão (100 μW ou menos), o que os torna mais indicados para sistemas de pequenas distâncias, baixo custo e média taxa de transmissão, devido à moderada largura de banda. Têm longa vida útil, baixo consumo de energia e são encontrados comercialmente nos comprimentos de onda desde o ultravioleta até o infravermelho. Já no caso dos lasers semicondutores, a luz é emitida a partir de emissão estimulada, com perfeita correlação de fase, frequência, polarização e direção de propagação entre a luz incidente e a luz emitida. Devido a essas características da emissão estimulada, os lasers são capazes de emitir a altas potências (100 *mW*), uma abertura angular estreita se comparada aos LEDs e uma largura espectral pequena, além de ser possível modular diretamente o laser semicondutor com altas taxas, até 25 *GHz* devido ao pequeno tempo de recombinação associado à emissão estimulada [1].

2.1.2

Modulação

De modo geral, para aplicação em qualquer tipo de sistema de comunicação, modulação pode ser definida como um processo que causa uma alteração controlada em um ou mais dos parâmetros básicos de um sinal, podendo ser modulação em amplitude (AM), em frequência (FM) ou em fase (PM), ou uma combinação destas. O sinal que contém a informação a ser transmitida, chamado de sinal modulador, gera uma variação no parâmetro de interesse do sinal da portadora, que é um sinal de alta frequência, proporcionalmente à variação do sinal modulador [28]. A figura 2.4 exemplifica o funcionamento da modulação em amplitude. As modulações em frequência e em fase obedecem ao mesmo fundamento, apenas com a diferença de qual parâmetro está sendo modulado. Após a recepção do sinal no destinatário, para reaver o sinal modulador e obter a informação original, é necessário fazer a demodulação, que é a separação da portadora e da moduladora. A demodulação será tratada na seção 2.3. Existem ainda outras formas de modulação que podem ser usadas em sistemas de radiofrequência e microondas, como, por exemplo, as modulações pulsadas: modulação por amplitude de pulso (PAM), modulação por largura de pulso (PWM), modulação por posição de pulso (PPM) e modulação por código de pulso (PCM), utilizando amostragem e quantização do sinal analógico a ser transmitido, como pode ser visto no esquemático da figura 2.5.

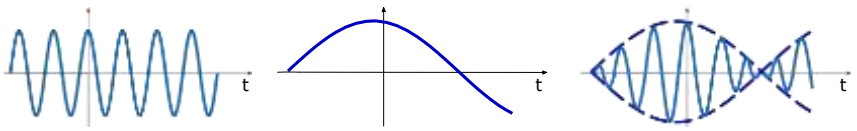


Figura 2.4: Exemplo de modulação em amplitude (AM). Em (a) é apresentada uma portadora senoidal, em (b) o sinal a ser transmitido e em (c) o sinal modulado, onde se verifica que a amplitude da portadora possui uma envoltória, correspondente ao sinal modulador.

Para aplicação em comunicações ópticas, as modulações AM, FM e PM são extensões óbvias dos sistemas convencionais de radiofrequência e microondas. Como consequência da frequência extremamente alta da portadora óptica, uma faixa espectral bastante larga está disponível e pode-se, em princípio, transmitir grandes quantidades de informação. Entretanto, a modulação do campo elétrico nas frequências da banda óptica é um tanto difícil de implementar por várias razões práticas, entre elas a necessidade de fibra óptica monomodo, devido ao grande ruído modal, um laser altamente coerente como fonte óptica, dificuldade de modulação direta de fase e de frequência, uma

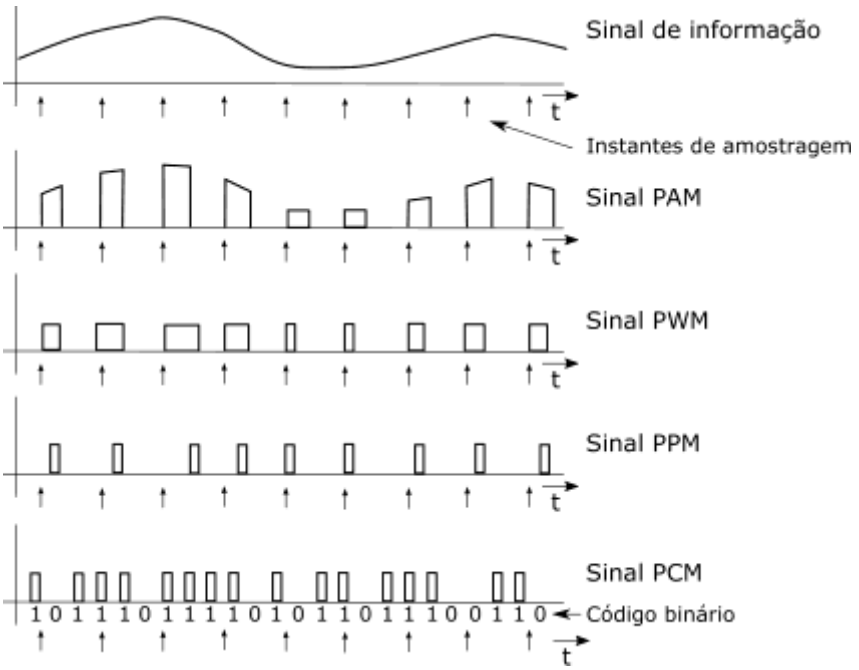


Figura 2.5: Esquemáticos das modulações pulsadas PAM, PWM, PPM e PCM de um sinal genérico.

forma de controlar e monitorar a polarização e um receptor capaz de medir a magnitude e a fase do campo óptico [27].

Já em um sistema de modulação de intensidade, o que é proporcional ao sinal que se deseja transmitir é a intensidade (ou potência) óptica. A potência óptica emitida pode ser variada facilmente ao se variar a corrente elétrica injetada em um LED ou em um laser semicondutor e a potência recebida pode ser medida diretamente. Como apenas a potência óptica é modulada e detectada, as oscilações de alta frequência do campo óptico não têm influência alguma no desempenho do sistema. A intensidade pode também ser facilmente modulada digitalmente ou em pulsos. Um importante método de modulação de intensidade da luz é o uso de PCM, onde a presença ou ausência de um pulso de luz representam, respectivamente, os bits 1 e 0. Este tipo de codificação é representado na figura 2.6 e é chamado de *On-Off Keying* (OOK), ou chaveamento liga-desliga.

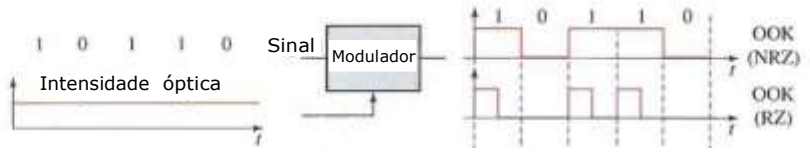


Figura 2.6: Exemplos de modulação da intensidade da luz em PCM sem retorno ao zero (NRZ-OOK) e com retorno ao zero (RZ-OOK).

Em comunicações quânticas, existem ainda outras formas de codificação

dos bits clássicos 1 e 0 em qubits, os bits quânticos. Pode-se codificá-los em qualquer estado quântico controlável e mensurável, sendo os mais simples de se conseguir na prática a polarização da luz e o *time-bin*, em que o instante de chegada dos fótons define a qual qubit ele corresponde. Estas formas de codificação e os qubits serão abordados de forma mais aprofundada na seção 3.1.

2.1.3
Acoplamento no Meio de Transmissão

Como já mencionado anteriormente, apenas parte da luz emitida em um material semicondutor escapa do material para o meio externo (ar) e pode ser utilizada como fonte óptica. Existem basicamente dois meios de transmissão óptica: o espaço livre e as fibras ópticas. Caso o meio de transmissão utilizado seja a fibra óptica, há ainda a necessidade de que a luz que escapa da fonte seja acoplada na fibra, o que, na prática, já é disponibilizado embutido no encapsulamento em fontes ópticas comerciais. Caso o meio de transmissão desejado seja o espaço livre, teoricamente a luz emitida por LEDs e lasers que escapa do material já se encontra em espaço livre. Porém, devido à fabricação dos dispositivos obtidos comercialmente, na grande maioria das vezes é necessário realizar o acoplamento da luz da fibra para o espaço livre.

A fibra óptica é um meio composto de um núcleo dielétrico transparente e flexível feito de sílica ou plástico e uma casca, cuja diferença de índice de refração faz com que a energia eletromagnética na faixa do espectro óptico da luz visível e do infravermelho seja confinada (reflexão interna total) em seu núcleo e possa ser transmitida a grandes distâncias. Como o índice de refração do núcleo (n_1) é maior que o índice de refração da casca (n_2), existe um ângulo crítico (θ_c), mostrado na figura 2.7(b), tal que toda a luz incidente na interface entre os meios com um ângulo de incidência maior que o ângulo crítico sofrerá reflexão, ao invés de refração, como visto na figura 2.7(c). O ângulo crítico pode ser calculado utilizando-se a lei de Snell ($n_1 sen\theta_1 = n_2 sen\theta_2$) e é aquele cuja luz refratada é paralela à interface entre os meios, ou seja, $\theta_2 = \pi/2$ [29].

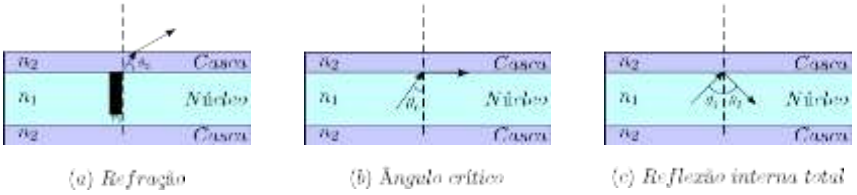


Figura 2.7: Refração da luz na interface entre os dois meios de uma fibra óptica.

O ângulo crítico é definido em relação à normal à interface entre os meios,

que, no caso da fibra óptica, é também normal ao eixo da fibra. O ângulo de aceitação, por outro lado, é definido em relação ao próprio eixo da fibra e representa o maior ângulo de acoplamento (θ_{max}) de um raio luminoso, tal que reflexão interna total ocorre na interface núcleo-casca dentro da fibra, como esquematizado na figura 2.8. O ângulo de aceitação completo é igual a $2\theta_{max}$ e a abertura numérica, que é o valor do seno do ângulo de aceitação, é definida pela equação (2-2), onde n_0, n_1 e n_2 são os índices de refração do ar, do núcleo da fibra e de sua casca, respectivamente.

$$NA = n_0 sen\theta_{max} = \sqrt{n_1^2 - n_2^2} \tag{2-2}$$

A abertura numérica é uma característica importante, pois determinamos, a partir dela, o cone de aceitação da fibra e a eficiência de acoplamento da luz. Adicionalmente, a fibra óptica atua como um guia de onda e pode propagar um número máximo de modos em seu núcleo. Entretanto, fibras ópticas monomodo são preferíveis para comunicações, pois é possível obter maiores taxas de transmissão e maiores distâncias quando comparadas a fibrasmultimodo [1]. Entre as grandes vantagens das fibras ópticas com relação a fios de cobre, estão sua baixa atenuação ($\approx 0,2 dB/km$), sua grande largura de banda, seu peso reduzido e a imunidade a interferência eletromagnética. Desta forma, as fibras ópticas conseguem transmitir informação com menos ruído e menos erros.

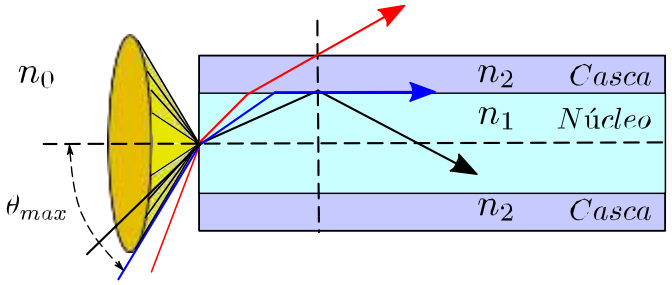


Figura 2.8: Ilustração do conceito de cone de aceitação e abertura numérica em fibras ópticas.

Os LEDs, que emitem luz incoerente, podem ser considerdos como fontes *Lambertianas* com distribuição angular $S(0) = S_0 cos\theta$, onde S_0 é a intensidade na direção $\theta = 0$. A eficiência de acoplamento para este tipo de fonte depende da abertura numérica da fibra e é dada por $\eta_c = (NA)^2$. Desta forma, apenas uma pequena parte da potência óptica emitida pelo LED é acoplada na fibra, uma vez que os valores típicos de NA para fibras multimodo são na faixa de $0,1$ *a* $0,3$ ($0,01 < \eta_c < 0,09$) [1].

Já no caso dos lasers, por sofrer emissão estimulada, a luz emitida é colimada, isto é, os feixes emitidos são ondas eletromagnéticas que se

progagam quase paralelamente entre si. Porém, uma seção reta elíptica e grande ângulo de divergência devido à difração na saída do semicondutor dificultam o acoplamento da luz à fibra de modo eficiente. Um conversor de seção reta (*spot-size converter*) é, às vezes, usado para melhorar a eficiência de acoplamento. Enquanto a eficiência de acoplamento de LEDs muda com a abertura numérica e pode se tornar $< 1\%$ no caso de fibras monomodo, a eficiência de acoplamento para lasers com emissão pela borda, em contraste, é tipicamente de $40 - 50\%$ e, no caso de VCSELs (*Vertical-Cavity Surface-Emitting Lasers* ou lasers de emissão de superfície de cavidade vertical), pode ultrapassar 80%, em função da seção reta do feixe ser circular e não elíptica. Normalmente, um pequeno pedaço de fibra (conhecido como rabicho ou *pigtail*) é incluído com o transmissor, de forma que a eficiência de acoplamento seja maximizada durante o encapsulamento. Uma emenda (*splice*) ou um conector é usado para unir o rabicho e o cabo de fibra óptica.

Para acoplar a luz da fibra óptica de volta ao espaço livre, a forma mais simples e eficiente é a utilização de um conjunto de lentes na extremidade de saída da fibra. Considerando que a luz emitida pela fonte óptica é acoplada na fibra ocupando todo o cone de aceitação, ela será emitida na outra extremidade, através da interface entre o núcleo da fibra e o ar, também ocupando o mesmo cone, o que caracteriza um feixe de luz divergente. Ao se colocar um conjunto de lentes adequado nesta extremidade, é possível colimar o feixe, inclusive escolhendo o melhor diâmetro para a aplicação desejada. Um conjunto de apenas duas lentes pode ser suficiente para atingir o objetivo.

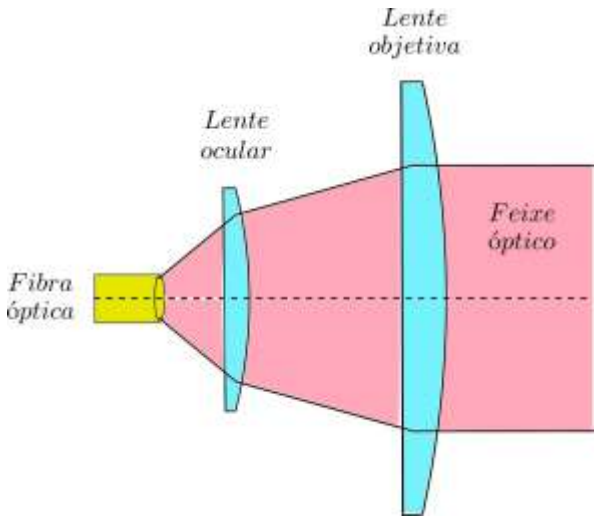


Figura 2.9: Esquemático de conjunto de duas lentes para transmissão em espaço livre.

Um exemplo de conjunto de duas lentes para transmissão em espaço livre é apresentado no esquemático da figura 2.9. A luz que se propaga dentro da

fibra óptica é refratada na interface entre a fibra e o ar e o feixe resultante é divergente, ocupando todo o ângulo sólido que compõe o cone de aceitação. Ao atingir a lente ocular, que é convergente, o feixe sofre nova refração, em uma primeira aproximação à colimação. A segunda lente, objetiva, também convergente, é capaz de colimar o feixe, que então se propaga no espaço-livre em direção ao receptor. Para que o feixe seja realmente colimado, é necessário o ajuste preciso da posição relativa das lentes entre si e em relação à extremidade da fibra. A posição correta das peças dependerá de suas distâncias focais, bem como da abertura numérica da fibra e pode ser calculada satisfatoriamente por óptica geométrica. Na prática, a lente ocular é encontrada comercialmente, já otimizada para uso com fibras ópticas, incluindo conector com rosca compatível com os conectores padrão comerciais de fibras e, portanto, apenas a lente objetiva deve ser projetada e ajustada para a colimação do feixe.

2.2
Meio de Transmissão – Atmosfera

A transmissão óptica em espaço livre (FSO), como o nome já diz, trata-se da transmissão de sinais ópticos pela atmosfera (ar) ou outro meio não guiado, como vácuo no caso de comunicações envolvendo estações espaciais ou água no caso de comunicações submarinas. Neste trabalho, o conceito de espaço livre é aplicado apenas à atmosfera, portanto, este é o meio a ser estudado. Interessantemente, a luz se propaga mais rápido pelo ar (≈ 300.000 *km/s*) do que pela sílica das fibras ópticas (≈ 200.000 *km/s*), então, pode-se classificar as comunicações ópticas em espaço livre (FSOC) como *comunicações ópticas na velocidade da luz* [30].

Ao contrário do cabo de fibra óptica, que é um meio previsível, o espaço livre é um meio de transmissão aberto, e, portanto, menos previsível. Devido a essa imprevisibilidade, é mais difícil controlar a transmissão óptica no espaço livre. Essa característica pode afetar a capacidade máxima de projeto, podendo até levar à indisponibilidade temporária do sistema.

FSO é uma tecnologia que necessita de linha de visada, o que significa que os pontos que se interconectam precisam poder se enxergar, sem nada obstruindo o caminho. Os principais causadores de dificuldades em FSO incluem névoa, absorção, espalhamentos, obstruções físicas (pássaros, por exemplo), balanço do edifício e cintilação. Assim, devemos sempre considerar vários fatores associados à atmosfera, que interferem na transmissão dos sinais ópticos, como: absorção da luz, não homogeneidade do meio, espalhamentos devido a moléculas gasosas ou partículas em suspensão, refração, turbulências, emissão de radiação pelos constituintes atmosféricos, cintilação, etc.

Basicamente, podemos verificar que a atenuação da radiação transmitida na atmosfera é dada pela soma da absorção com os espalhamentos: ATENUAÇÃO = ABSORÇÃO + ESPALHAMENTOS. A Lei de Beer (equação (2-3)) descreve a transmissão (τ) da luz se propagando em espaço livre em termos de espalhamento e absorção em função da distância x.

$$I_R/I_0 = \tau = exp(-\gamma x) \tag{2-3}$$

onde $\gamma = \alpha_m + \alpha_a + \beta_m + \beta_a$ é o coeficiente de atenuação, dado pela soma dos coeficientes de espalhamento molecular (α_m), espalhamento por aerossóis (α_a), absorção molecular (β_m) e absorção por aerossóis (β_a), I_R/I_0 é a razão entre a intensidade detectada (I_R) e a intensidade inicialmente transmitida (I_0). Cada um dos coeficientes de espalhamento e de absorção é uma função do comprimento de onda.

Outro fator que influencia na qualidade do sinal recebido é o ruído. Dentre as fontes de ruído, o sol é o contribuinte mais importante, pois sua energia, além de poder ser absorvida diretamente pelo sistema receptor, origina vários fenômenos ao interagir com os materiais da superfície da Terra, tais quais a reflexão, a absorção, a transmissão, a luminescência, o aquecimento, etc. Esses materiais emitem ou reemitem a energia absorvida. Assim, existem também ruídos gerados pela radiação emitida pelos diversos materiais no entorno do enlace [26]. Todos estes fenômenos serão brevemente discutidos nas próximas seções.

2.2.1 Espalhamento

O espalhamento pode influenciar drasticamente o desempenho de sistemas FSO, porém, ele não é relacionado a uma perda de energia. Na realidade, ele se refere à energia sendo desviada para outro lugar que não o receptor do sistema, o que pode causar uma redução significativa na intensidade da luz efetivamente recebida. O regime de espalhamento que ocorrerá com o feixe de luz de comprimento de onda λ depende do tamanho das partículas presentes no caminho da luz. Uma descrição pode ser dada por um parâmetro de tamanho, x_0, adimensional. A equação que o descreve é $x_0 = 2\pi r/\lambda$, onde r é o raio da partícula presente na atmosfera. Para $x_0 \ll 1$, ou seja, quando a partícula é muito pequena em comparação ao comprimento de onda, o espalhamento predominante será o de Rayleigh, causado pelas moléculas dos gases existentes na atmosfera; para $x_0 \approx 1$, ou seja, quando a partícula espalhadora é da mesma ordem de grandeza do comprimento de onda da luz, o predominante é o espalhamento de Mie; e para $x_0 \gg 1$, espalhamento não-seletivo ou geométrico [30].

2.2.1.1
Espalhamento Rayleigh

Este regime de espalhamento ocorre quando a radiação incide nos elétrons ligados aos átomos ou moléculas. Esta radiação induz um dipolo que oscila na frequência da radiação incidente. Os elétrons oscilantes emitem luz nesta mesma frequência, mas em uma direção aleatória. O espalhamento Rayleigh varia com λ^{-4} e esta dependência associada ao tamanho das partículas presentes na atmosfera implicam que os menores comprimentos de onda sofrem mais espalhamento que os maiores. Espalhamento Rayleigh é a razão pela qual o céu parece azul sob condições de tempo ensolarado. Para sistemas FSO operando com comprimento de onda na faixa do infravermelho próximo, o impacto do espalhamento Rayleigh no sinal de transmissão pode ser desprezado, como pode ser depreendido do gráfico da figura 2.10, que exibe a dependência da seção transversal do espalhamento Rayleigh com o comprimento de onda para a faixa espectral do infravermelho.

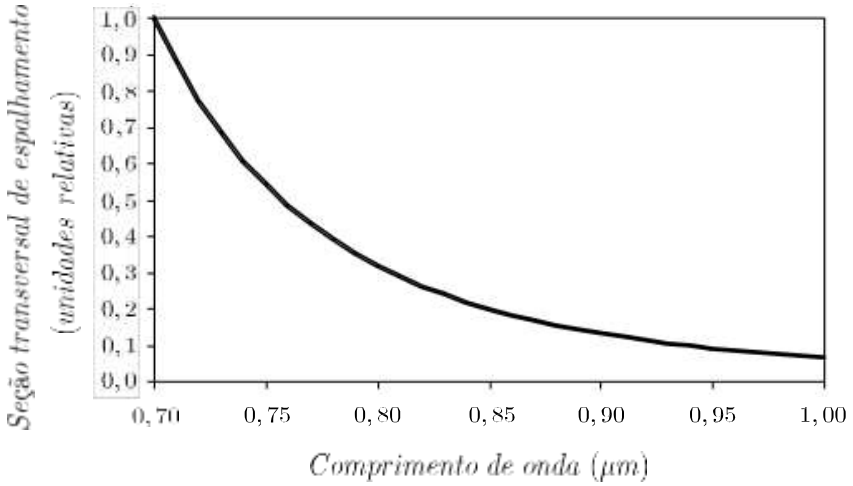


Figura 2.10: Seção transversal de espalhamento Rayleigh *versus* comprimento de onda [30].

2.2.1.2
Espalhamento Mie

O espalhamento Mie é o mecanismo de espalhamento dominante quando as partículas presentes na atmosfera têm tamanho da mesma ordem de grandeza do comprimento de onda utilizado. As partículas de névoas, neblinas e aerossóis (poluição) têm raio médio próximo ao comprimento de onda comumente utilizado em FSO; por este motivo, são os principais elementos

de preocupação quanto ao espalhamento Mie, ao contrário da chuva e da neve, cujas partículas apresentam raios médios maiores. Entretanto, as partículas de névoas, neblinas e aerossóis podem ter tamanhos variados, dependendo das condições climáticas, o que torna necessário realizar um cálculo detalhado da atenuação causada por espalhamento Mie, que leva em conta a distribuição estatística do tamanho das partículas espalhadoras. Há algumas fórmulas empíricas para o cálculo dessa atenuação, mas elas não se aplicam igualmente em diferentes tipos de névoa.

A teoria é complicada, mas bem compreendida. O problema surge ao se tentar comparar a teoria a um experimento. A absorção domina a maior parte do espectro, desta forma, os dados devem ser coletados em faixas de comprimento de onda que ocorrem em uma janela atmosférica, com a suposição de que apenas o espalhamento está ocorrendo. Além disso, a distribuição de partículas deve ser bem conhecida. Para aerossóis, essa distribuição depende da localização, tempo, umidade relativa, velocidade do vento e assim por diante. Simulações numéricas da fórmula exata de espalhamento de Mie sugerem que o coeficiente de atenuação não depende drasticamente do comprimento de onda na faixa do infravermelho próximo normalmente usada em sistemas FSO. A conclusão geral que pode ser derivada da observação empírica é que o espalhamento de Mie causado pelo nevoeiro é a principal fonte de atenuação do feixe e que esse efeito é acentuado geometricamente à medida que a distância é aumentada. Para todos os fins práticos, as condições de visibilidade na área de implantação do FSO devem ser estudadas.

2.2.1.3 Espalhamento Geométrico

Este tipo de espalhamento ocorre quando os raios das partículas em suspensão na atmosfera são muitos maiores do que o comprimento de onda, pode ser descrito utilizando-se óptica geométrica e é independente do comprimento de onda da luz. Esse é o caso, por exemplo, da atenuação por chuvas, que afeta todos os comprimentos de onda da mesma forma. Com relação à luz visível, podemos observar espalhamento independente do comprimento de onda nas nuvens, que em dias de céu claro são brancas [31]. O espalhamento não seletivo ocorre nas camadas mais baixas da atmosfera e é causado principalmente por poeira, gotas d'água, fragmentos de gelo, nevoeiro e nuvens, com partículas em geral com secções transversais maiores que dez vezes o comprimento de onda comumente utilizado em FSO. Tais partículas refletem toda a radiação incidente e, desta forma, quando se apresentam em formações muito densas,

agem como uma obstrução física entre os dois pontos do enlace, impedindo, ou ao menos dificultando muito, a transmissão dos sinais ópticos.

2.2.1.4
Condições Climáticas

Como dito anteriormente, a chuva tem um impacto redutor de distância em sistemas de FSOC, embora este seja menor que o do nevoeiro, porque os raios das gotas de chuva (200 a 2000 *μm*) são muito maiores que os comprimentos de ondas típicos usados em FSO.

A atenuação típica da chuva é geralmente moderada. Por exemplo, para uma chuva de 25 *mm/h*, a atenuação aproximada é de 4 *dB/km* (ver tabela 2.1). Em áreas metropolitanas, onde as distâncias dos edifícios são usualmente menores que 1 *km*, a atenuação esperada devido à chuva tende a ser menor que 4 *dB*. Entretanto, quando a chuva aumenta consideravelmente, chegando a mais de 100 *mm/h*, o espalhamento causado pelas gotas pode se tornar um problema em instalações com distâncias maiores que as típicas em áreas urbanas. Todavia, essas chuvas mais fortes normalmente duram pouco tempo, questão de minutos.

Já os flocos de neve são cristais de gelo que vêm em uma variedade de formas e tamanhos. Em geral, no entanto, a neve tende a ser maior que a chuva, o que faz com que a dispersão não costume ser um grande problema para os sistemas FSO.

Como já mencionado, o nevoeiro é o fenômeno climático mais prejudicial para os links de FSOC. As condições meteorológicas são normalmente referidas como nevoeiro quando as visibilidades variam entre 0 e 2000 metros. Como as condições de nevoeiro são um pouco difíceis de descrever por meios físicos, palavras descritivas como “nevoeiro denso” ou “nevoeiro fino” são algumas vezes usadas para caracterizar a aparência dele. Quando a visibilidade é superior a 2000 *m*, a condição é frequentemente referida como neblina.

Mesmo condições modestas de nevoeiro podem atenuar altamente os sinais infravermelhos em distâncias mais curtas. A atenuação esperada em *dB/km* e sua correlação com a visibilidade são mostradas na tabela 2.1. A tabela também ilustra claramente que a chuva tem muito menos impacto nas perdas de percurso dos sistemas FSO quando comparada à neblina. Por exemplo, uma precipitação média resulta em menos atenuação que um nevoeiro fino.

Como o nevoeiro ainda não é muito bem entendido, é difícil caracterizá-lo fisicamente e a visibilidade é mais comumente utilizada para caracterizar as

Tabela 2.1: Código internacional de visibilidade para condições climáticas e precipitação.

Condições Climáticas	**Precipitação**	**Quantidade (*mm/h*)**	**Visibilidade**	**Perda (*dB/km*)**
Nevoeiro Denso			0 *m*, 50 *m*	271, 65
Nevoeiro Espesso			200 *m*	59, 57
Nevoeiro Moderado ou Neve			500 *m*	20, 99
Nevoeiro Leve ou Neve	Temporal	100	770 *m*	12, 65
			1 *km*	9, 26
Nevoeiro Fino ou Neve	Chuva Forte	25	1, 9 *km*	4, 22
			2 *km*	3, 96
Neblina ou Neve	Chuva Moderada	12, 5	2, 8*km*	2, 58
			4*km*	1, 62
Neblina Leve ou Neve	Chuva fina	2, 5	5, 9 *km*	0, 96
			10 *km*	0, 44
Céu Limpo ou Neve	Chuvisco	0, 25	18, 1 *km*	0, 24
			20 *km*	0, 22
Céu Muito Limpo			23 *km*	0, 19
			50 *km*	0, 06

condições de nevoeiro, ainda que outros métodos, como tamanho médio das partículas e medidas de densidade sejam também usadas. A comunidade do FSO utiliza principalmente dados de visibilidade porque essas medidas foram tomadas nos principais aeroportos por muitas décadas. Até certo ponto, tais medidas permitem caracterizar regiões diferentes e derivar valores estatísticos de disponibilidade para sistemas FSO.

Microclimas ambientais, como lagoas e rios, podem induzir condições de nevoeiro ou neblina, logo, os dados coletados nos aeroportos às vezes não são confiáveis para ambientes próximos. No entanto, foi demonstrado que a visibilidade nos aeroportos fornece uma boa estimativa para o valor mínimo de disponibilidade esperado. Isso ocorre porque os aeroportos geralmente estão localizados fora dos limites metropolitanos e o microclima dentro de uma cidade geralmente gera menos condições de neblina e nevoeiro.

Para a maioria dos enlaces comerciais FSO, a operação em ambientes de nevoeiro pesado requer manter as distâncias entre os terminais transceptores as mais curtas possíveis para manter os níveis de disponibilidade elevados. As margens de potência do enlace da maioria dos equipamentos vendidos permitem disponibilidades que excedem 99, 99% se as distâncias forem mantidas

abaixo de 200 *m*.

2.2.1.5 Turbulência

Poderíamos pensar, então, na instalação de sistemas FSO em desertos. Em regiões quentes e secas, os fenômenos de espalhamento descritos anteriormente são desprezíveis. Porém, um outro fenômeno surge para atrapalhar os sistemas de FSOC: a turbulência. A terra e o ar se aquecem, mas não uniformemente. Alguns bolsões (ou células) de ar se formam, por aquecerem mais do que suas vizinhanças, fazendo com que haja uma variação do índice de refração na trajetória percorrida pelo feixe de luz, o que, por sua vez, altera o trajeto do feixe. Devido a estas bolsas de ar não serem estáveis no tempo ou no espaço, a mudança do índice de refração parece seguir um movimento aleatório. É possível perceber este efeito na faixa do comprimento de luz visível ao olharmos em direção ao horizonte ao longo de uma rua ou estrada, em dias muito quentes e secos. Isto aparece como distorção e movimento da imagem no horizonte com relação à posição original fixa e/ou com uma aparência de que tem um bolsão d'água no ar, ao longo do caminho.

Pode-se observar três efeitos distintos causados em um feixe de laser sob a turbulência. Primeiro, o feixe pode excursionar aleatoriamente através dos bolsões de ar devido às várias mudanças do índice de refração ao longo de sua trajetória. Este é um fenômeno conhecido como *beam wander*. A refração através de meios tais como o ar trabalha similarmente como a passagem em qualquer outro tipo de meios de refração, tais como uma lente de vidro, logo, a luz será focalizada ou desfocalizada aleatoriamente, depois das mudanças do índice ao longo do trajeto de transmissão. Segundo, a fase do feixe pode variar, produzindo flutuações da intensidade ou *cintilações*. E, por fim, o feixe pode sofrer espalhamentos maiores do que os previstos pelos tipos de espalhamentos já abordados aqui.

Dos três efeitos da turbulência, a cintilação é o que mais afeta os sistemas de transmissões ópticas em espaço livre. Interferências aleatórias com a frente de onda podem causar picos e quedas da intensidade, tendo por resultado a saturação ou a perda do sinal do receptor. Pontos de calor na seção transversal do feixe podem ocorrer do tamanho $\sqrt{\lambda L}$, ou seja, aproximadamente 4 *cm* para um feixe de 1550 *nm* em 1 *K m* percorrido, ou 1, 5 *cm* para apenas 160 *m* percorridos, que é o caso da realização experimental deste trabalho.

Para minimizar os efeitos da cintilação no trajeto da transmissão, os sistemas FSOC não devem ser instalados perto de superfícies quentes. Por

exemplo, os telhados recobertos com mantas de piche ou telhados de zinco, que podem ocasionar uma quantidade elevada de cintilação em dias quentes de verão, não são pontos preferenciais para instalação dos enlaces. Como a cintilação diminui com a altura (distância vertical entre os objetos aquecidos e o trajeto do feixe), o melhor seria que os sistemas de FSOC fossem instalados um pouco mais acima do telhado ($> 1,2\ m$) e afastado das paredes laterais da edificação para evitar ser atingido pela canalização das massas de ar quente que escorregam para cima pressionadas contra as paredes dos prédios [26]. É prudente, ainda, que na instalação dos sistemas FSOC, o percurso do feixe deva estar a mais de 5 *m* acima das ruas da cidade ou de outras fontes potenciais de cintilações mais severas.

Nos capítulos 3 e 5 veremos que, devido às características quânticas inerentes a este trabalho, ele foi realizado com baixíssimas potências de laser, com uma média da ordem de poucos fótons por pulso (idealmente um fóton), dentre os pulsos que contém fótons, e, portanto, a turbulência terá o efeito de desviar este fóton para fora do alvo, o que será interpretado pelo receptor como um pulso vazio, exatamente o mesmo efeito que os outros tipos de espalhamento.

Ademais, o efeito *beam wander* tem baixa taxa de flutuações (em torno de 1 KHz a 2 KHz), tal que um sistema de seguidor ativo simples pode ser usado para compensar as flutuações. Manter um feixe estreito na mira do detector pode não ser um problema por causa deste efeito.

2.2.2
Absorção

As partículas são caracterizadas pelo seu índice de refração. A parte imaginária do índice de refração (k) é relacionada ao coeficiente de absorção (α) por:

$$\alpha = \frac{4\pi k}{\lambda} = \sigma_a N_a \qquad (2\text{-}4)$$

Onde σ_a é a seção transversal de absorção e N_a é a concentração das partículas absorventes. Em outras palavras, o coeficiente de absorção é uma função da "força de absorção" de um dado tipo de partícula e da densidade desta partícula.

Na faixa de comprimentos de onda comumente utilizados em FSOC, podemos definir as *janelas atmosféricas de transmissão* como aquelas faixas de comprimento de onda fora daqueles em que os absorvedores componentes da atmosfera absorvem de forma significativa o feixe luminoso. O espectro típico de absorção atmosférica é ilustrado na figura 2.11. As partículas absorventes

mais comuns na constituição da atmosfera são água, dióxido de carbono e ozônio.

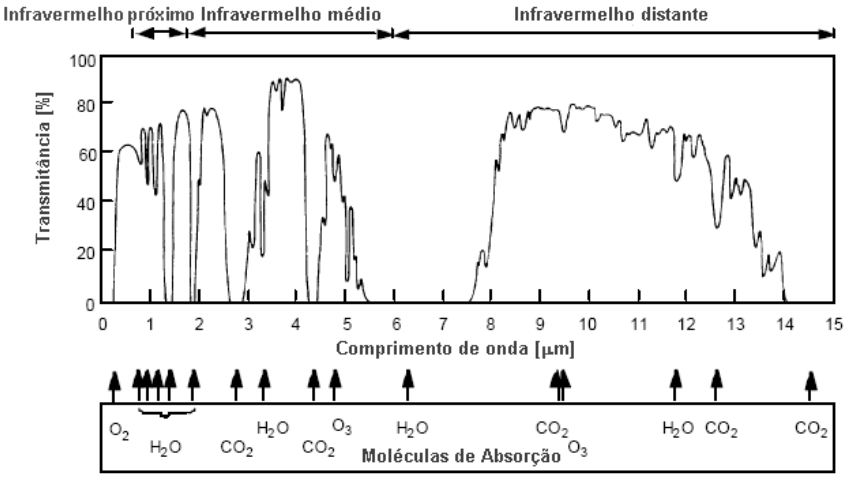


Figura 2.11: Janelas atmosféricas relativas às moléculas presentes na atmosfera [26].

Comumente, a absorção é dividida em dois tipos: a chamada absorção molecular, onde os fótons são absorvidos pelas próprias moléculas componentes da atmosfera fora das janelas de transmissão conhecidas e a absorção por aerossóis, que é definida como a absorção da luz por partículas sólidas ou líquidas em suspensão na atmosfera com distribuições aleatórias, como poeira, poluição, nevoeiro, neve, etc. Os estados vibracionais e rotatórios da energia destas partículas são capazes da absorção em muitas faixas do espectro. As janelas mais conhecidas estão entre $0,72$ e $15,0$ μm, algumas com limites estreitos [30].

O que determina o quanto o sinal será atenuado é a quantidade de absorventes na atmosfera. A figura 2.12 mostra o espectro simulado da transmissão para condições desobstruídas do céu com uma concentração urbana padrão de aerossol, vapor d'água e dióxido de carbono que fornece uma visibilidade média de 5 $K m$.

No infravermelho próximo, comprimentos de onda abaixo de 2 μm, o vapor de água é o absorvente molecular principal causador dos vales de absorção presentes no gráfico, com muitos traços para atenuar o sinal, como pode ser depreendido se analisarmos em conjunto a figura 2.13, que mostra o gráfico da simulação para absorção somente de vapor d'água em regime de céu limpo. As transições vibracionais e rotatórias determinam quais energias serão facilmente absorvidas, mas o grande número de permutações aumenta extremamente o número de traços. O comprimento de onda do laser utilizado neste trabalho ($1,55$ μm) situa-se exatamente nesta região.

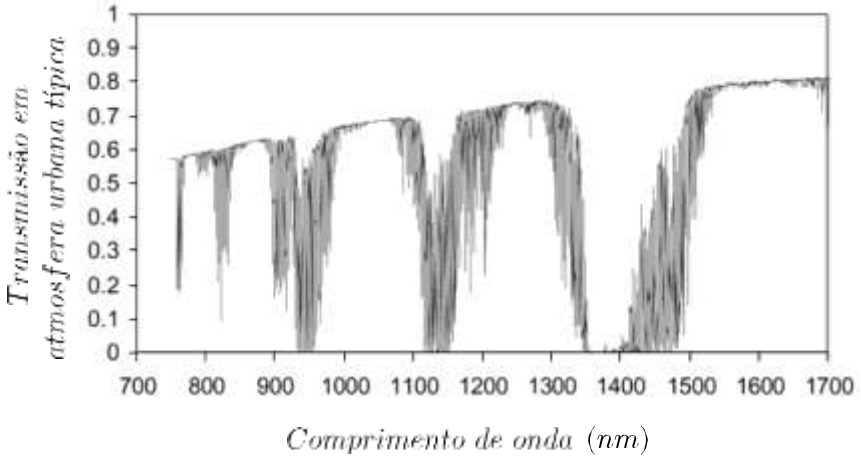


Figura 2.12: Simulação, em MODTRAN (software da *U.S. Air Force*), da transmissão em função do comprimento de onda em ambientes de aerossóis urbanos (visibilidade – 5 *K m*) [30].

Pode-se ver que, fora dos vales de absorção, a transmissão tem valor muito próximo de 1, o que significa que a absorção da luz pelo vapor d'água é quase inexistente nestas regiões, inclusive na janela de 1550 *nm* utilizada neste trabalho.

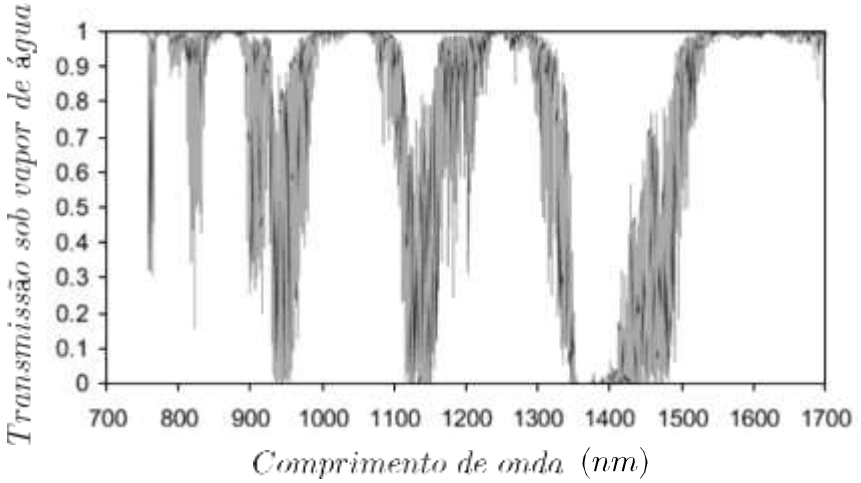


Figura 2.13: Simulação, em MODTRAN, da transmissão em função do comprimento de onda em ambiente com vapor d'água. [30].

A figura 2.14 mostra a transmissão de dióxido de carbono sob céu limpo. Percebemos que picos ressonantes agudos ocasionais são sobrepostos a um fundo geral relativamente plano.

Os aerossóis são partículas que podem advir de duas origens distintas: (a) ocorrem naturalmente na forma de poeira de meteoritos, partículas de sal marinho, poeira do deserto e detritos vulcânicos, ou (b) são criados como resultado da conversão química de gases residuais pelo homem em partículas

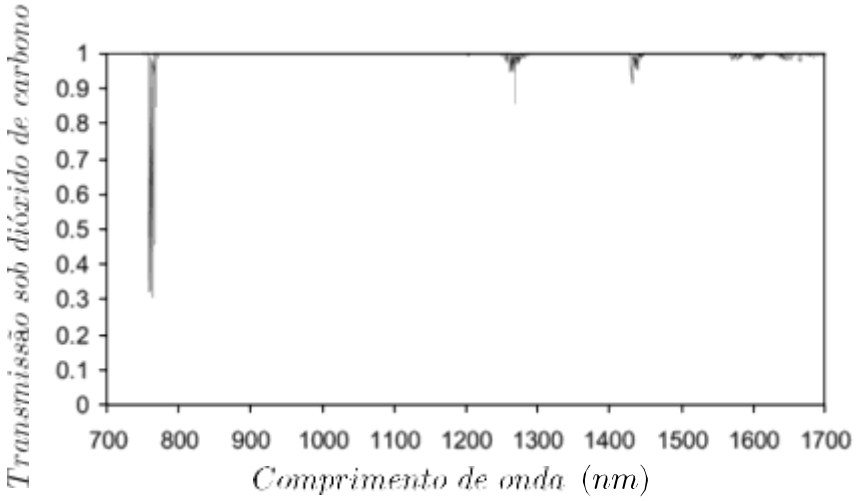


Figura 2.14: Simulação, em MODTRAN, da transmissão em função do comprimento de onda em ambiente com dióxido de carbono. [30].

sólidas e líquidas e como resíduo industrial. O tamanho dos aerossóis pode variar desde poeira fina, com menos de 0,1 μm de raio, até partículas gigantes, de raios maiores que 10,0 μm. Segundo [30], G. L. Stephens publicou em 1994 uma estimativa que determinou que 80% da massa de aerossol está contida no quilômetro mais baixo da atmosfera, que terra produz mais aerossóis que o oceano e que o Hemisfério Norte produz 61% da quantidade total de aerossóis no mundo. Os aerossóis provocam bastante *espalhamento* nos comprimentos de onda do espectro infravermelho, devido aos tamanhos dos raios das partículas atravessarem todos os comprimentos de onda deste espectro, o que pode definitivamente ser um problema para os sistemas FSO. No entanto, essas partículas *também absorvem* os comprimentos de onda infravermelhos, como pode ser visto na simulação da figura 2.15. Ainda observando a figura, nota-se a monotonicidade do efeito de absorção dos aerossóis nos comprimentos de onda entre 800 *nm* e 1700 *nm*. Não há picos ou vales no gráfico, mas apenas uma atenuação geral em todos os comprimentos de onda do intervalo, com a transmissão variando de 0,6 a 0,8.

Uma comparação das figura 2.15 com as figuras 2.14 e 2.13 mostra como a transmissão da atmosfera é afetada por partículas de aerossol. No comprimento de onda da janela de comunicações ususal de 1550 *nm*, podemos ver que o vapor d'água e o dióxido de carbono apresentam influência desprezível de absorção, enquanto os aerossóis urbanos comuns são os responsáveis por quase toda a atenuação do sinal por absorção.

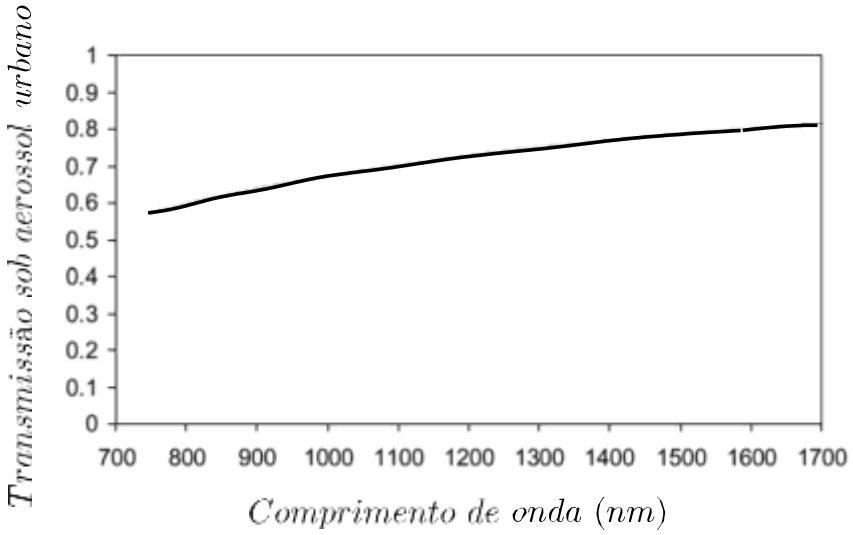


Figura 2.15: Simulação, em MODTRAN, da transmissão em função do comprimento de onda em ambiente com aerossóis urbanos. [30].

2.2.3
Ruídos

No final do século XIX, a área mais excitante da física era determinar os mecanismos da *radiação de corpo negro*, que foi o nome dado à "radiação de temperatura-pura", ou radiação resultante de um sistema em equilíbrio térmico. Como essa é a fonte fundamental do ruído eletromagnético primário (sol, estrelas, plasmas, etc.) e do secundário (lua, planetas, atmosfera etc.) e, além disso, foi algo tão básico no desenvolvimento da teoria quântica, trataremos o assunto de forma breve para dar uma pequena noção da natureza dessas fontes de ruído. Na sequência, abordaremos a influência da luz solar nos sistemas FSO.

2.2.3.1
Emissão dos Materiais – A Radiação de Corpo Negro

Toda substância com temperatura superior a zero absoluto ($0K$ ou $-273^{\circ}C$) emite radiação eletromagnética como resultado de suas oscilações atômicas e moleculares, conforme definido pela lei de radiação de corpos negros de Planck. Antes de discorrermos sobre as características e efeitos desse tipo de radiação, vamos mostrar brevemente como Planck chegou à descrição dela.

Por volta do ano 1900, após trabalhos teóricos independentes de Stefan-Boltzmann, Wien e Rayleigh-Jeans, e do trabalho experimental de Lummer e Pringsheim, o conhecimento sobre a radiação de corpo negro estava no seguinte estágio [32]:

1. A fórmula de Wien era assintoticamente correta para as altas frequências;

2. A fórmula de Rayleigh-Jeans era assintoticamente correta para as baixas frequências;

3. A dependência funcional de T_0 (com λT_0 constante) era conhecida (onde T_0 é a temperatura em Kelvin);

4. A energia total como função de T_0 era conhecida; e

5. Uma medida experimental precisa da função já tinha sido feita.

A figura 2.16 mostra a relação entre as fórmulas teóricas e os resultados experimentais, que, posteriormente, derivaram na lei de Planck.

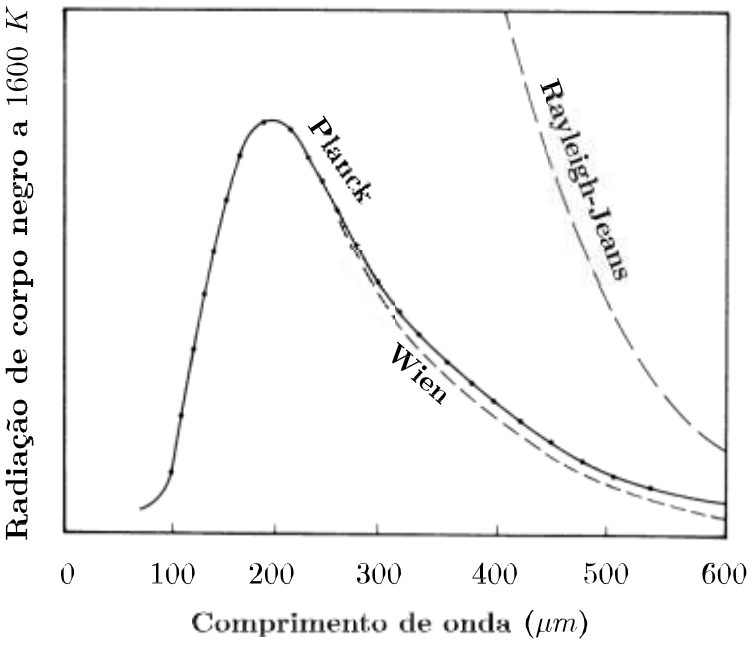


Figura 2.16: Gráficos das fórmulas de Wien, Rayleigh-Jeans e dos resultados experimentais.

A derivação de Planck da equação correta para a lei da radiação de corpo negro veio através de seu entendimento da termodinâmica. Ele ajustou a segunda derivada da entropia em relação à energia com a curva experimental para produzir as duas formas assintóticas corretas e fez "engenharia reversa" a fim de obter a equação da energia.

A resposta foi tão precisa que era claramente a fórmula correta. Planck então se propôs a obter um modelo experimental pelo qual pudesse desenvolver essa equação a partir de princípios básicos, mais uma vez usando a termodinâmica. Ele assumiu que a energia total consistia em um número finito de quantidades incrementais distribuídas aleatoriamente, e que a emissão e a absorção de radiação ocorriam não continuamente, mas em saltos de energia fixa (as quantidades incrementais): tratava-se da primeira suposição quântica!

A fórmula de Rayleigh-Jeans para a energia da radiação de corpo negro derivou do valor que Jeans havia calculado para o número de modos por ciclo:

$$D_{BB} = \frac{8\pi f^2}{c^3} \quad \therefore \quad E = kT_0 \frac{8\pi f^2}{c^3}$$

onde k é a constante de Boltzmann e f é a frequência da radiação. A derivação mais usada multiplica a densidade de modo D_{BB} pelo equivalente quântico de kT_0, que leva a:

$$\varphi_f = \frac{8\pi hc T_0^5}{(\lambda T_0)^5} \frac{1}{e^{hc/k\lambda T_0} - 1} \tag{2-5}$$

que se ajusta exatamente à curva medida; h é chamado constante de Planck ($h = 6,62607004 \times 10^{-34} m^2 kg/s$), e a energia incremental existe em quantidades integrais de hf. Observe que, integrando a equação (2-5), obtemos exatamente a lei de Stefan-Boltzmann. E, se derivarmos a equação (2-5) em relação a λ e resolvendo para o máximo valor, chegamos exatamente à lei de Wien.

Assim, vemos que a radiação de corpo negro pode ser caracterizada completamente por um único número que reflete a temperatura da fonte em seu valor máximo de emissão. Portanto, é bastante comum especificar todas as fontes por sua temperatura efetiva de corpo negro, porque, por mais enganosa que seja, essa temperatura de corpo negro produz uma potência comparável na mesma largura de banda.

2.2.3.2 A Influência do Sol

Embora as fontes de corpo negro tenham imensa importância teórica no campo da física, na verdade ela não ocorre tão naturalmente. Talvez a fonte que mais se assemelhe a um corpo negro e exista na natureza seja o sol. A intensidade solar medida fora da atmosfera apresenta grande semelhança a um corpo negro correspondente de 5900 K, com exceção dos comprimentos de onda muito curtos.

O gráfico da figura 2.17 mostra a dependência do ruído térmico (radiação de corpo negro) e da radiação solar com o comprimento de onda, supondo $T = 300K$ (temperatura ambiente aproximada da Terra) e assumindo valores realistas de fator de qualidade constante de 8000, que corresponde a um filtro de largura $\Delta\lambda = 0,1\ nm$ a $800\ nm$. A eficiência de detecção foi considerada constante e igual a 1 para todos os pontos da curva. A escala da curva azul (sólida) encontra-se no lado direito do gráfico, enquanto a escala da curva vermelha (tracejada), do lado esquerdo.

Note que o ruído térmico é extremamente alto para maiores comprimen-

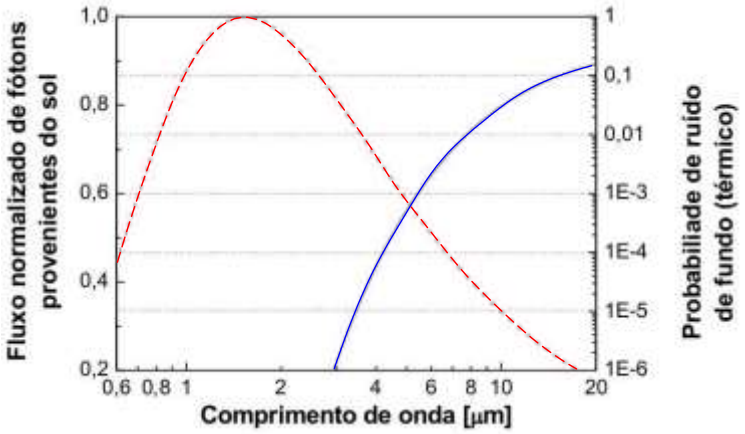


Figura 2.17: Linha sólida: probabilidade de ruído de fundo por pulso, em função do comprimento de onda. Linha tracejada: radiação solar normalizada, expressa em fótons por unidade de tempo por unidade de área por unidade de ângulo sólido [31].

tos de onda, acima de 20 *μm*, chegando a ultrapassar os 15%, mas que a curva decresce quase exponencialmente e que, a um comprimento de onda de 3 *μm*, o ruído já é 5 ordens de grandeza menor. A curva vermelha, que mostra o fluxo normalizado de fótons provenientes do sol, é dada por $(2/\lambda^2)(exp[hc/\lambda kT] - 1)^{-1}$. A escala nesse caso é linear, portanto não há diferença significativa entre os diferentes comprimentos de onda mostrados no gráfico com relação à radiação solar, mas observa-se que, para o infravermelho próximo e para luz visível, a fonte de ruído predominante é a luz do sol. O Sol emite radiação distribuída continuamente numa faixa que vai dos raios-x até a região de microondas, embora concentrado no intervalo de 350 *nm a* 2500 *nm*, ou seja, dentro do mesmo espectro usualmente utilizado nos enlaces de FSOC comerciais.

Quando capturamos uma energia de espaço livre através de um detector de luz infravermelha sem filtragem, este sinal adquirido, na maioria das vezes, é em grande parte a radiação proveniente do Sol, que interage com a atmosfera até atingir diretamente o receptor.

Os sistemas FSO usam filtros ópticos de banda estreita para minimizar o efeito da luz solar direta. Se possível, os sistemas a laser não devem ser montados em uma orientação direta leste-oeste para evitar os efeitos da luz solar direta, pois, estando ela na frente da unidade, pode resultar em períodos curtos de tempo em que o receptor ficará inoperante devido à saturação do fotodiodo do receptor. Essas interrupções podem durar vários minutos, dependendo da época do ano e do ângulo do sol no céu. No entanto, devido ao campo de visão estreito da óptica receptora, o sol deve aparecer quase

diretamente atrás da cabeça do link para que isso aconteça. Portanto, a luz do sol é potencialmente um problema durante os primeiros minutos da manhã, em horário próximo ao por do sol ou se uma das extremidades do link apontar sob um ângulo agudo para o céu. O sistema se recuperará completamente depois que o sol estiver fora do campo de visão do receptor. Para enlaces instalados em áreas urbanas, poderá haver outros horários em que a luz do sol tem grande influência no desempenho do sistema, a depender dos corpos refletores no entorno do enlace. A luz do sol indireta, refletida nesses objetos, pode ser intensa o suficiente para gerar ruído significativo no sistema receptor, como o exemplo que pode ser visto na janela indicada pela seta vermelha na figura 2.18. Nesta foto, o fotógrafo estava a poucos centímetros de distância do canhão receptor.

Figura 2.18: Foto realizada no local de instalação do receptor. É possível ver o reflexo concentrado da luz do sol na janela de um edifício próximo.

A maioria dos fornecedores de sistemas FSO comerciais incorpora filtros de bloqueio da luz solar de banda estreita que minimizam drasticamente o impacto da luz solar direta.

A tabela 2.2 mostra a comparação da intensidade solar ao nível do mar para condições de tempo seco e úmido com algumas outras fontes de luminosidade. Note que, na óptica, quando dizemos "tão diferentes quanto noite e dia", queremos dizer 60 *dB*. Essa é a diferença entre a intensidade solar e a intensidade da lua cheia, como pode ser observado da tabela.

Sob condições de iluminação noturna, as fontes de ruído óptico dominantes são a radiância do céu causada por fontes zodiacais, galácticas e de fontes de luz celeste espalhada [32]. A lua e os planetas também podem contribuir

Tabela 2.2: Ordem de magnitude da intensidade de várias fontes de luz ao nível do mar [32].

Condições de Luminosidade	**Intensidade (W/m^2)**
Dia claro	10^3
Dia pouco nublado	10^2
Dia muito nublado	10
Interiores muito bem iluminados	1
Irradiação lunar da lua cheia	10^{-3}
Irradiação de estrela de primeira magnitude	10^{-8}

para o ruído recebido. Mas, como iremos mostrar no capítulo 5, a filtragem do ruído proveniente da luz do sol é tão eficiente que garante que os ruídos gerados à noite (seis ordens de grandeza menores que durante o dia) não têm qualquer influência no sistema e, portanto, não serão abordados neste trabalho.

2.3 Sistemas Receptores

O projeto de um receptor óptico depende da escolha de modulação usada pelo transmissor, mas, independente da forma, a função de um receptor óptico é converter o sinal óptico de volta à forma elétrica e recuperar a informação transmitida. Funciona de forma analogamente inversa ao transmissor. Embora o enlace FSO utilize basicamente uma fonte de luz modulada para enviar o sinal, o receptor muitas vezes acaba detectando esse sinal somado a algumas componentes indesejáveis na forma de interferências ou ruídos. Assim, o receptor deve, basicamente, captar o sinal do meio de transmissão, filtrar os ruídos, demodular e apresentar de alguma forma a informação recebida. O seu principal componente é o fotodetector, que converte luz em eletricidade por meio do efeito fotoelétrico. Os requisitos para um fotodetector são similares àqueles para uma fonte óptica: alta sensibilidade, resposta rápida, baixo ruído, baixo custo e alta confiabilidade. Tais requisitos são mais bem atendidos por fotodetectores feitos de materiais semicondutores.

O receptor pode ser projetado de duas formas: o fotodetector pode ser colocado na captação do sinal óptico vindo do meio de transmissão ou no final do processo, como o último elemento do sistema. No primeiro caso, o sinal óptico é captado do meio, convertido em sinal elétrico pelo fotodetector e então o processamento todo feito eletricamente. No segundo caso, o sinal é captado do meio, tratado por componentes ópticos no sistema e só então, quando tratado e separado da portadora, convertido para informação no domínio elétrico pelo fotodetector. O primeiro caso, processamento de sinais elétricos, é tema de

estudo exaustivamente tratado na literatura. Ademais, neste trabalho usamos um tratamento do sinal óptico e, ao convertê-lo por meio de fotodetectores, ele já possui significado (bits 0 ou 1), sendo necessária apenas uma conciliação de informações entre dois detectores diferentes, em lugar de um processamento propriamente dito. Assim, apenas o segundo caso será tratado nesta seção.

2.3.1
Captação do Sinal do Meio Óptico

A maioria dos componentes ópticos encontrados comercialmente são desenvolvidos para uso com fibras ópticas. Desta forma, para o tratamento óptico do sinal, se o meio de transmissão for a fibra óptica, basta conectá-la de forma padrão aos equipamentos no receptor, sem maiores preocupações. Já a melhor forma de captar o sinal transmitido em espaço livre é acoplá-lo à fibra óptica e então utilizar as mesmas conexões que no caso anterior.

Para o acoplamento com a fibra óptica, é necessário convergir o feixe para que ele tenha o diâmetro menor ou igual ao da fibra e que o ângulo de incidência dos raios esteja dentro da abertura numérica. Obviamente, raios incidentes fora da interface ar-núcleo não entram na fibra e raios incidentes na interface, mas fora do cone de aceitação, não serão acoplados, pois não sofrerão reflexão interna total na interface núcleo-casca da fibra, como explicado na seção 2.1.3. Todo o raciocínio e as fórmulas apresentadas naquela seção são válidos também para o receptor. Uma vez que o diâmetro típico das fibras multimodo (de 50 a 125 μm) é maior que o típico para fibras monomodo (10 μm), o acoplamento da luz em fibras multimodo é mais fácil de ser obtido na prática e, na maioria dos casos, pode ser usado no receptor o mesmo sistema de lentes usado no transmissor, desde que a distância entre eles não seja grande o suficiente para que o feixe não possa mais ser considerado colimado devido à divergência, como esquematizado na figura 2.19. Mas, mesmo no caso de maiores distâncias, em que o feixe diverge, a solução pode ser obtida pela colocação de uma lente colimadora à frente do sistema. A depender da magnitude do diâmetro do feixe, entretanto, pode ser que o tamanho necessário para essa lente a torne uma solução inviável.

No projeto do canhão transceptor, além da preocupação com o diâmetro do feixe e do ponto focal a fim de acoplar o máximo possível de energia na fibra óptica, deve-se ter atenção à escolha da orientação e do formato das lentes quanto à correção de aberrações. Para melhorar o desempenho do sistema, os projetistas ópticos devem garantir que a contribuição total da aberração de todas as superfícies tomadas em conjunto seja quase zero. Normalmente, esse processo requer análise computadorizada e otimização. No entanto, existem

algumas diretrizes simples que podem ser usadas para conseguir isso com lentes disponíveis em catálogo, utilizando-se combinações de lentes com aberrações positivas e lentes com aberrações negativas. Um excelente guia sobre este assunto pode ser encontrado em [33].

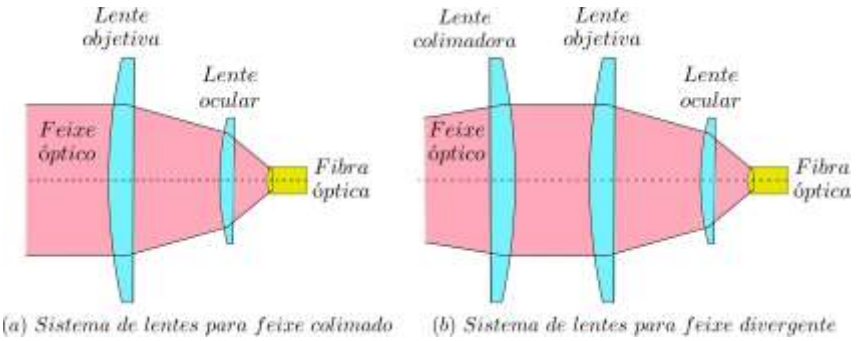


Figura 2.19: Esquemático de sistema genérico de lentes para receptor óptico de espaço livre com acoplamento em fibra óptica.

2.3.2 Filtragem

O projeto dos filtros utilizados em sistemas de comunicação depende de quais tipos de ruídos e interferências estão presentes no canal. Nos sistemas de FSOC, a maior fonte de ruído é a luz do sol, seja ela direta ou refletida em algum objeto, como vimos na seção 2.2.3.

Para que a luz do sol gere ruídos na detecção, em primeiro lugar ela deve ser captada pelo sistema de lentes e, em segundo lugar, conseguir acoplar na fibra óptica do detector. Para que isto ocorra, o sol, ou o objeto que reflete sua luz, deve estar no campo de visão do sistema receptor e a luz deve incidir na interface com a fibra óptica dentro de sua abertura numérica. Devido ao pequeno campo de visão típico dos sistemas de FSOC, a própria posição do sol já funciona como uma espécie de "filtro natural" para o sistema. Entretanto, a energia do sol captada em determinadas horas do dia, em que o sol está em frente ao elemento receptor ou o sol está em alguma posição em que sua luz refletida em determinado objeto está localizada, como uma fonte secundária, em frente ao receptor, a filtragem implementada no sistema deve agir.

Na subseção 2.2.3.2, vimos que o sol emite luminosidade nos comprimentos de onda desde raios-x até microondas, mas concentrado na região entre 350 *nm* a 2500 *nm*, que é justamente a região típica dos detectores de sistemas de FSO. Assim, precisamos filtrar de alguma forma a luz solar nestes comprimentos de onda.

Figura 2.20: Foto de um filtro óptico de espaço livre disponível no laboratório. Sua aparência é semelhante à de uma lente.

A opção mais viável, então, é acoplar a energia luminosa na fibra óptica e utilizar uma rede de Bragg para filtrar a luz em comprimento de onda. Uma rede de Bragg gravada em uma fibra óptica constitui uma modulação local e periódica do índice de refração do núcleo da fibra, como exemplificado na figura 2.21. Normalmente, utilizam-se fibras com alta concentração de germânio. A rede de Bragg opera como um filtro espectral reflexivo que seleciona uma faixa estreita de comprimento de onda de uma banda larga de comprimentos de onda que tenham sido acoplados à fibra.

Este comprimento de onda, chamado de comprimento de onda de Bragg (λ_B) está relacionado com a periodicidade espacial da modulação do índice de refração (Λ) e com o índice de refração efetivo do núcleo (n_{eff}) através da equação:

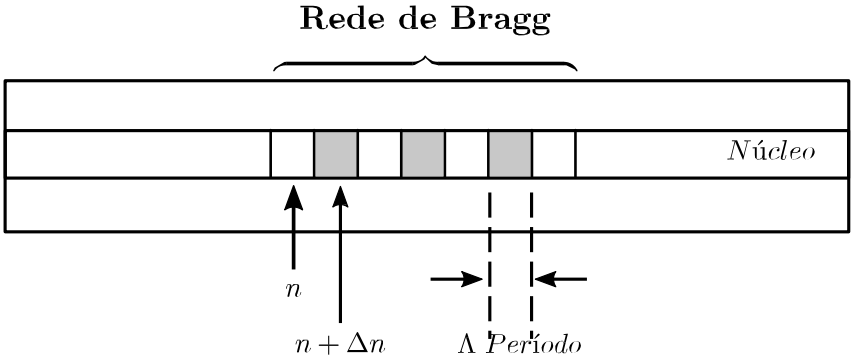


Figura 2.21: Esquema da construção de uma rede de Bragg em uma fibra óptica.

$$\lambda_B = 2n_{eff}\Lambda \tag{2-6}$$

Na figura 2.22 é representada uma rede de Bragg centrada em $\lambda_B = 700\,nm$ (vermelho) sendo iluminada por uma fonte de luz de banda espectral larga na faixa do visível e infravermelho próximo (que é representado na figura pela faixa roxa após o vermelho no espectro). Uma faixa estreita do espectro de luz, centrada em λ_B, é refletida, e o restante do espectro é transmitido.

A rede de Bragg não filtrará 100% da luz solar, mas, tendo em vista que só não serão filtrados pela rede de Bragg os comprimentos de onda de 1550 *nm* (±0,55 *nm* – que é a largura de banda da rede de Bragg aqui utilizada), a quantidade de luz solar não-filtrada será pequena e, em geral, a relação sinal-ruído será boa, quanto mais se somarmos o "filtro natural" mencionado anteriormente. Esta afirmação pode ser verificada verdadeira ao se analisarem os resultados apresentados na seção 5.5.

Em resumo, para a luz solar (direta ou indireta) ser detectada, ela deve ter comprimento de onda casado com λ_B, o comprimento de onda da rede de Bragg, deve se originar no campo de visão do detector, atingir a extremidade da fibra óptica com um ângulo dentro da abertura numérica da fibra, alcançar o elemento fotossensível do detector (ver seção 2.3.4) e não ser perdida devido à ineficiência do detector. É de se esperar que a eficiência desta filtragem seja suficiente para termos um sistema no mínimo viável.

O uso do filtro traz ainda uma vantagem adicional: filtros impedem ataques do tipo "cavalo de tróia" em sistemas QKD [34].

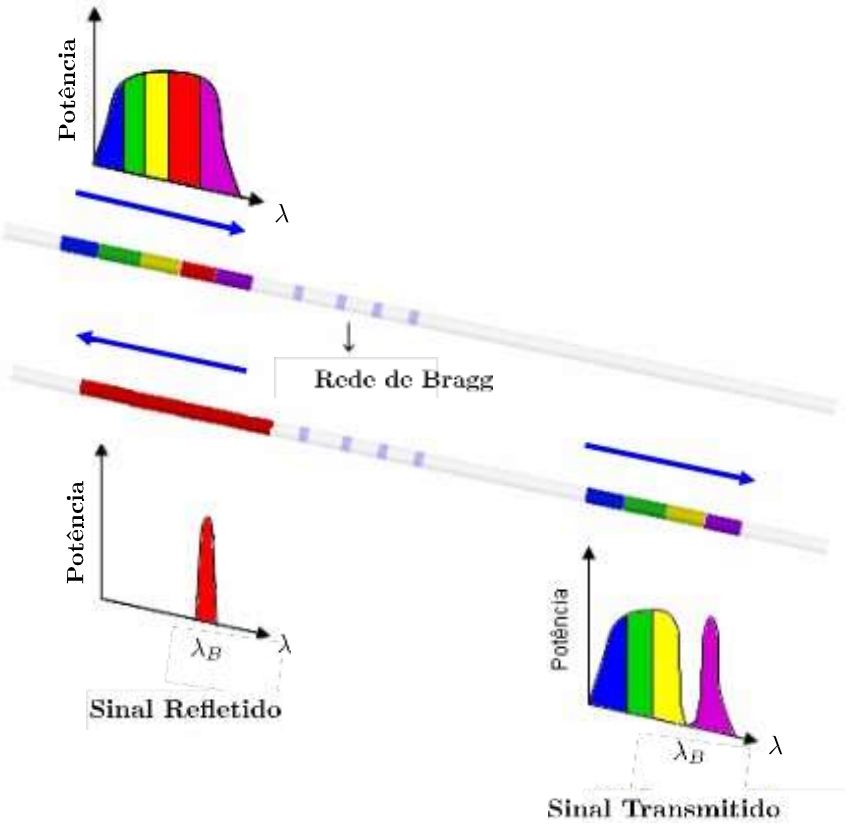


Figura 2.22: Esquema do princípio de operação de uma rede de Bragg em fibra óptica. Uma faixa estreita do espectro de luz, centrada no comprimento de onda de Bragg (λ_B) é refletida, e o restante do espectro é transmitido.

2.3.3 Demodulação

Demodulação pode ser definida como o processo de recuperação do sinal original (ou até da informação contida nele, caso não seja necessário um decodificador no sistema) a partir da separação da onda moduladora e da onda portadora e é o processo inverso à modulação. Portanto, ela é diretamente dependente e definida a partir daquele processo. Existem muitos tipos de modulação (ver seção 2.1.2), logo, existem muitos tipos de demodulação. Obviamente, se o sinal foi modulado em amplitude, por exemplo, não podemos implementar demodulação de frequência. Neste caso, somente a demodulação de amplitude cumprirá o objetivo de extrair a informação original.

Usualmente, em sistemas de comunicação, o processo de demodulação é realizado por um sistema eletrônico. Os circuitos de demodulação variam de algo tão simples quanto um detector de pico modificado a algo tão complexo quanto a conversão descendente em quadratura coerente combinada com algoritmos sofisticados de decodificação executados por um processador de sinal digital. Muitas técnicas, como recuperação de portadora, recuperação

de clock, *bit slip*, sincronização de quadros, compressão de pulso, indicação de intensidade de sinal recebido, detecção e correção de erros, e outras, são executadas por demoduladores, embora qualquer demodulador específico possa executar apenas algumas ou nenhuma dessas técnicas.

Para comunicações ópticas, a demodulação pode ser implementada de outra forma que não o circuito eletrônico: a demodulação por equipamentos ópticos. Um exemplo é o caso da modulação em intensidade óptica, em que o próprio detector óptico já opera como um demodulador, na medida em que é capaz de detectar diretamente a intensidade óptica. Outro exemplo é a modulação em frequência, em que pode ser usado um multiplexador por divisão de comprimento de onda (WDM[1]) para separar a portadora e a moduladora. Neste caso, há a necessidade da colocação de um decodificador após o demodulador.

No caso de comunicações quânticas, há, ainda, outras formas de demodulação. Para codificação em *time-bin*, a capacidade do próprio detector de identificar o instante de chegada dos fótons já funciona como demodulador, uma vez que extrai a informação original (qubit[2] $|0\rangle$ ou $|1\rangle$, representando bits clássicos "0" e "1") separada do portador (fóton). Para codificação em polarização, um divisor de feixe polarizador (PBS) separa os qubits diferentes em canais diferentes, em que cada tipo de qubit será detectado por um detector diferente. Desta forma, o PBS age como demodulador, enquanto a conciliação de informação entre os detectores funciona como decodificador.

2.3.4 Detecção

Nos mecanismos de detecção óptica, os fótons interagem diretamente com os elétrons em um material. Quase sempre o material utilizado é um material semicondutor. Como os elétrons podem ser ligados a átomos da rede, a átomos de impureza ou podem ser livres, é possível uma variedade de interações. Podem ser classificados em mecanismos internos e externos (foto-emissivos). Os mecanismos internos podem ser ainda subdivididos em excitação de portadores adicionais, em que os fótons interagem com elétrons ligados a átomos, formando pares buracos-elétrons (fotocondutividade, efeito fotovoltáico, efeito fotoeletromagnético, efeito *Dember* e fototransistor), interações com portadores livres (*photon drag*, *hot electron bolometer* e detector *Putley*) e interações

[1] Um WDM é um dispositivo com um entrada óptica e diversas saídas. Cada saída permite a passagem de luz em um comprimento de onda específico, funcionando como um filtro para os outros comprimentos de onda. Assim, a luz da entrada no WDM é separada em diferentes comprimentos de onda em cada saída.

[2] Para notação de Dirac, ver o apêndice A de [31] e para significado de qubit ver seção 3.1.

localizadas, em que os fótons incidentes produzem uma excitação localizada nos elétrons, sem retirá-los dos átomos (contador quântico IR, fósforo e filme fotográfico). Os mecanismos externos, por sua vez, podem ser subdivididos em foto-catodos (convencional e afinidade de eletronegatividade) e mecanismos de ganho (avalanche de gás, foto-multiplicadores e *channel electron multiplication*).

Um detector óptico é simplesmente um material fotossensível que responde à luz incidente liberando fotoelétrons. Variações na intensidade da luz causam variações semelhantes no número de elétrons liberados. Os parâmetros importantes de comunicação que caracterizam os fotodetectores são a eficiência quântica do material fotossensível (ou responsividade), ganho, largura de banda e corrente de escuro. A eficiência quântica de um material fotossensível é formalmente definida como a probabilidade de um fóton incidente gerar um fotoelétron:

$$\eta = \frac{\textit{potência do campo óptico detectado}}{\textit{potência do campo óptico incidente}} \tag{2-7}$$

A *eficiência* η mede a capacidade do material fotossensível de detectar potência de campo incidente convertendo-a em corrente e é, via de regra, dependente do comprimento de onda (ou frequência) incidente.

Se mais de um elétron for coletado na saída (devido a geração secundária interna) quando um fotoelétron inicial (primário) é liberado do material fotossensível, a sensibilidade do detector é aumentada. Assim, se G elétrons são coletados para cada fotoelétron primário, a corrente de saída é amplificada pelo fator G. Este último é chamado de *ganho* do fotodetector, e vemos que é relacionado à capacidade do detector de fornecer fotomultiplicação interna. Esse ganho interno pode ser obtido de emissões eletrônicas secundárias ou por recombinações eletrônicas no próprio fotodetector.

A *largura de banda* de base de um fotodetector é a frequência mais alta à qual o material fotossensível consegue responder. Portanto, são as variações de potência de campo que podem ser detectadas como variações de corrente de saída. Como tal, a largura de banda do detector determina o limite superior de frequência ao qual um campo de intensidade modulada pode ser fielmente detectado. Os detectores ópticos geralmente têm larguras de banda de vários *GHz*.

Corrente de escuro é um fluxo de corrente de saída que aparece mesmo na ausência de luz incidente e é causado por emissão aleatória do material do detector devido apenas à energia térmica inerente. A corrente de escuro aparece como um fluxo de corrente que varia aleatoriamente sobre um valor médio $\boldsymbol{I}_{dc}$ de corrente. Este último é frequentemente chamado de corrente de escuro média do

detector. As variações aleatórias sobre o valor médio da corrente são devidas à natureza do ruído de disparo das emissões e, portanto, têm uma dependência de variação também proporcional a I_{dc}. Como a corrente de escuro é um fenômeno induzido termicamente, geralmente pode ser reduzida pelo resfriamento do detector. Esse efeito se torna mais um problema no infravermelho, onde os comprimentos de onda das portadoras estão mais próximos dos comprimentos de onda naturais associados à emissão do corpo negro a 300 K.

Os fotodetectores são de quatro tipos básicos, dependendo de sua construção e mecanismos de fluxo de elétrons. O *detector de tubo de vácuo* (fototubo) contém um vácuo através do qual os elétrons, liberados de um material fotoemissivo em resposta à luz incidente, viajam para serem coletados no anodo. Seu tamanho é o típico da maioria dos tubos de vácuo. O fotodiodo, ou diodo PIN, é um dispositivo semicondutor que utiliza a luz incidente em uma junção p–n para liberar elétrons. Tais dispositivos podem ter milímetros de tamanho e ter eficiências relativamente altas, com a largura de banda limitada por tempos de recombinação de elétrons na transição do gap p–n. *Tubos fotomultiplicadores* (PMT) são tubos de vácuo que produzem fotomultiplicação através de emissões secundárias de dinodos internos, dentro do tubo de vácuo e, portanto, têm ganho inerente. Como vários desses dinodos podem ser inseridos em fototubos padrão, o ganho do PMT é geralmente bastante grande (10^4 a 10^8). O *fotodetector de avalanche* (APD) é um dispositivo fotodetector semicondutor que utiliza dopagem de gap para desencadear mais geração de elétrons livres a partir de um elétron primário inicial (avalanches) para produzir ganho. Os APDs são pequenos em tamanho e seus valores de ganho úteis são limitados à faixa de 50 a 200. Valores de ganho mais altos causam instabilidade de ganho e sensibilidade a variações de potência do circuito de polarização.

Um problema básico com qualquer dispositivo fotomultiplicador é que o número de elétrons gerados secundariamente a partir de um elétron primário é, na verdade, aleatório. Isto significa que o ganho G de tais dispositivos é, de fato, uma variável aleatória, com densidade de probabilidade do ganho, média do ganho $\overline{G}$, etc. Porém, como este trabalho se baseia no uso de detector de fótons únicos por avalanche, o valor preciso da corrente gerada por cada avalanche não é importante, visto que cada uma delas, independente do valor da corrente gerada, é interpretada como uma, e somente uma, detecção. Mais detalhes sobre este tipo de detector são discutidos nas seções 3.4 e 4.1.

Uma das medidas clássicas do desempenho de um receptor de comunicação é a *relação sinal-ruído* (SNR) detectada. Este parâmetro é simplesmente a razão entre a potência média do sinal detectado e a potência do ruído total adicionado a ele. Como tal, o SNR é uma medida das potências relativas

do sinal e do ruído detectados e serve como uma indicação da capacidade do receptor de coletar o campo óptico desejado.

O parâmetro SNR indica o efeito das várias fontes de ruído na capacidade de detecção do receptor. Um receptor óptico geralmente recebe uma designação especial, dependendo de quais termos tendem a dominar: limitado pelo ruído térmico, limitado pela corrente de escuro, limitado pelo ruído de fundo, limitado pelo ruído quântico [32]. O SNR máximo ocorre sob condições de ruído quântico e a principal interferência é causada apenas pelo ruído de disparo do próprio sinal. Em operação limitada por ruído de fundo, por ruído térmico ou por corrente de escuro, o SNR varia com o quadrado da potência do sinal recebido, mas varia linearmente quando a condição de limitação quântica é atingida.

O ganho médio $\overline{G}$ do detector reduz diretamente o efeito do ruído térmico na contribuição para o SNR de saída. Portanto, a fotodetecção de alto ganho é desejada em receptores ruidosos. No entanto, uma vez que a operação com limitação por contagem de escuro é alcançada, não há vantagem em ganho adicional. O SNR está sempre diretamente relacionado a $\alpha = \eta/hf$, onde η é a eficiência do detector e, portanto, sempre desejamos detectores altamente eficientes. A eficiência do detector, no entanto, depende da frequência, assim como da intensidade do ruído de fundo, de modo que o SNR está implicitamente relacionado ao comprimento de onda óptico específico utilizado.

3
Comunicações Quânticas

Chamamos de "Comunicações Quânticas" uma sub-área da teoria da informação quântica que lida com a transmissão, propagação e detecção dos portadores quânticos da informação, os chamados *quantum bits* ou *qubits*. O conceito do qubit é, talvez, o que há de mais revolucionário no advento da teoria da informação quântica. Embora ele não seja nada mais que um sistema quântico de dois níveis, assim como o bit clássico é um sistema clássico de dois níveis, o qubit forneceu, pela primeira vez, uma interpretação física para a informação, e o nome passou a ser usado tanto para descrever o grau de liberdade (de 2 níveis) no qual a informação foi codificada, como para também descrever o próprio portador da informação. Para comunicações de longas distâncias, a radiação eletromagnética é a candidata mais natural para se implementar qubits, e o fóton surge como "partícula elementar" de comunicações quânticas. Esse fato oferece uma posição extremamente privilegiada a todos os grupos de pesquisa do mundo que trabalham na área de óptica – ou, mais especificamente, óptica quântica.

Este capítulo tem como objetivo fazer uma breve introdução ao assunto e apresenta, inicialmente, o conceito de qubit, bem como suas características principais. Na sequência, são discutidos os componentes básicos de sistemas de comunicações ópticas: a pseudo-fonte de fótons únicos, o canal quântico e os detectores quânticos. Por fim, os conceitos de criptografia quântica e amplificação de privacidade são explorados na última seção do capítulo.

3.1
O Qubit

Na teoria da informação, a entidade fundamental é o bit e, para representá-lo, pode-se usar qualquer sistema físico que possua dois estados distintos para codificar a informação nos bits "0" e "1", como, por exemplo, um espelho refletindo a luz do sol em direção a um observador, que pode se encontrar nos estados "ligado" (refletindo em direção ao observador) ou "desligado" (refletindo em qualquer outra direção ou não refletindo). Outro exemplo é o uso de duas frequências sonoras audíveis diferentes f_1 e f_2 para representar os bits "0" e "1".

Na teoria da informação quântica, utilizamos um ente análogo ao bit, com diversas similaridades com este, apesar de serem muito diferentes: o "qubit", que pode ser definido como se segue:

Definição 1 *Um qubit é um vetor de estado em um espaço de estados bidimensional, ou seja, um vetor unitário* $|\Psi) \in H$, *onde* H *é um espaço de Hilbert complexo de dimensão 2 [31].*

Em outras palavras, um qubit é um estado qualquer de um sistema quântico de duas dimensões[1]. Embora essa definição seja suficiente para caracterizar um qubit, ela oferece pouca intuição. Talvez a ideia fique mais clara ao se fazer uma analogia com os "zeros" e "uns" dos bits, o que é feito na próxima sub-seção.

3.1.1
A Representação dos Qubits

A forma mais usual de representar o qubit é como combinação linear de certa base ortonormal (*base computacional*), representada pelos kets $|0)$ e $|1)$. A base está normalmente associada a um dos observáveis que representam o conjunto de medidas que podem ser realizadas nos qubits. A cada componente da base atribuímos os valores clássicos $0 \rightarrow |0)$ e $1 \rightarrow |1)$ (Atenção para não confundir o ket $|0)$ com o vetor nulo).

Como um exemplo, pode-se representar os qubits por um sistema atômico de dois níveis, em que o estado fundamental do átomo representaria $|0)$ e o estado excitado representaria o $|1)$, o que é muito semelhante à representação clássica, por exemplo, em dois níveis de tensão elétrica, cujo nível alto representa o bit "1" enquanto o nível baixo representa o bit "0". A grande diferença entre o sistema quântico e o sistema clássico é que aquele pode se encontrar em uma superposição entre os dois estados, ou seja, pode estar em um combinação linear dos dois estados $|0)$ e $|1)$. Desta forma, a descrição de um qubit genérico pode ser dada por:

$$|\Psi) = \alpha|0) + \beta|1) \tag{3-1}$$

onde α e β são números complexos que representam as amplitudes de probabilidade de se medir cada um dos valores, ao medi-los na base computacional, isto é,

$$p(\text{"0"}) = |(0|\Psi)|^2 = |\alpha|^2 \; ; \quad p(\text{"1"}) = |(1|\Psi)|^2 = |\beta|^2 \tag{3-2}$$

[1]Para uma introdução aos espaços de Hilbert e à notação de Dirac usada para os qubits, ver o apêndice A de [31].

onde $|\alpha|^2 + |\beta|^2 = 1$. Como pode ser inferido, um qubit pode assumir quaisquer valores intermediários entre "0" e "1" em um espaço contínuo parametrizado pelos coeficientes α e β, pois ele é dado por uma superposição coerente entre dois estados quânticos. Um exemplo é o qubit dado por

$$|\Psi) = \frac{1}{\sqrt{2}}(|0) + |1)) \tag{3-3}$$

que, se for medido na base computacional, apresenta 50% de chance de ser medido como "0" e 50% de chance de ser medido como "1". De certa forma, o qubit é "0" e "1" ao mesmo tempo, o que parece estranho à primeira vista, mas é perfeitamente normal pelas leis da física quântica.

Ao mesmo tempo, se aplicarmos uma *transformação de Hadamard* (H) à base computacional, verificamos que, de certa forma, o mesmo qubit definido na equação (3-3) sempre possui valor definido. Se representarmos o bit "0" pelo ket $|+45)$ e o bit "1" pelo ket $|-45)$, podemos reescrever:

$$\begin{aligned} 0 \rightarrow |+45) &= H|0) = \frac{1}{\sqrt{2}}(|0) + |1)) \\ 1 \rightarrow |-45) &= H|1) = \frac{1}{\sqrt{2}}(|0) - |1)) \end{aligned} \tag{3-4}$$

Não é difícil perceber que, nesta base, o qubit definido na equação (3-3) tem valor bem definido e igual a 0. Do ponto de vista experimental, entretanto, nem sempre é simples realizar uma mudança de base como essa, como, por exemplo, no caso do átomo de dois níveis.

Para a visualização do espaço em que os qubits se encontram, podemos utilizar a *esfera de Bloch* (também conhecida como *esfera de Poincaré,* devido à associação com a esfera de representação dos estados de polarização da luz[2]), em que os infinitos estados possíveis são representados pelos infinitos pontos na superfície da esfera, sendo os estados ortogonais representados em pontos diametralmente opostos. Na esfera exemplificada na figura 3.1, os polos norte e sul da esfera representam, respectivamente, os estados $|0)$ e $|1)$.

Embora a quantidade de informação clássica necessária para se descrever um qubit seja infinita, só podemos extrair 1 bit clássico de informação. Infelizmente, a "informação infinita" contida em um qubit está indisponível ou, mais precisamente, nos é inacessível, pois não podemos obter nenhuma informação sem realizar uma medida e qualquer medida realizada terá como resultado um dos auto-estados $|0)$ ou $|1)$.

[2]Para estudo da esfera de Poincaré, seção 6.1 de [27].

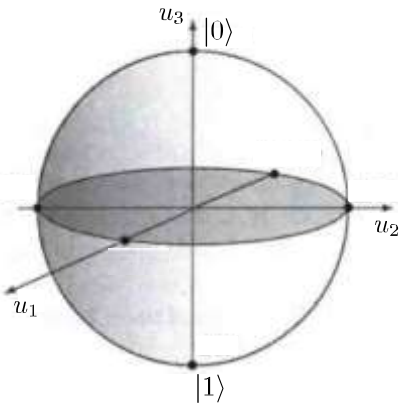


Figura 3.1: Representação dos qubits como pontos na superfície da esfera de Bloch.

3.1.2 Múltiplos Qubits

Sempre podemos escrever uma sequência de bits clássicos, como, por exemplo, "001" ou "1101", logo, temos que poder representar também um conjunto de *n* qubits. Cada qubit é representado por um sistema físico distinto e, portanto, o estado global deve ser representado por um produto tensorial entre os estados individuais.

$$|\Psi) = |\Psi_1)|\Psi_2) \ldots |\Psi_n) \tag{3-5}$$

Onde a notação simplificada para o produto tensorial foi utilizada e seu símbolo ($\otimes$) é omitido. Cada qubit pertence a um espaço de Hilbert diferente e, portanto, o conjunto de qubits representado pertence ao estado de Hilbert resultante, da mesma forma, do produto tensorial entre os estados individuais: $|\Psi) \in H_1 \otimes H_2 \otimes \ldots \otimes H_n$.

Depreende-se da equação (3-5) que um conjunto de qubits $|\Psi)$ pode se encontrar em uma superposição de todas as possíveis combinações dos estados mensuráveis $|0)$ e $|1)$ dos qubits $|\Psi_n)$ que compõem o conjunto, assim como um qubit pode se encontrar em uma superposição dos dois estados mensuráveis. Por exemplo, se $|\Psi) = |0)|0)$, a aplicação da transformação de Hadamard da equação (3-4) a cada qubit resulta em

$$\begin{aligned} H|0) \otimes H|0) &= \frac{1}{\sqrt{2}}(|0) + |1)) \otimes \frac{1}{\sqrt{2}}(|0) + |1)) \\ &= \frac{1}{2}(|0)|0) + |0)|1) + |1)|0) + |1)|1)) \end{aligned} \tag{3-6}$$

que é uma superposição de todos os 4 possíveis valores clássicos "0" e "1". Esse resultado pode ser naturalmente estendido para mais de 2 qubits:

a aplicação de uma mesma transformação em n qubits pode resultar em uma superposição de todos os 2^n possíveis valores. Podemos interpretar esse fato como uma primeira vantagem de um computador quântico sobre um computador clássico, que é normalmente chamada de *paralelismo quântico*: se o registrador se encontrar em uma superposição de todos os valores possíveis, uma tarefa (digamos, calcular os valores de uma função para todas as entradas possíveis) pode ser realizada em um tempo exponencialmente mais curto que em um computador clássico.[3]

3.1.3 Implementações Práticas do Qubit

Apesar de qualquer sistema quântico de dois níveis poder ser utilzado para representar qubits, nem todos são de fácil implementação. Um elemento que apresenta diversas características que podem ser utilizadas como sistemas de dois níveis é o fóton, até mesmo pela facilidade de transmiti-lo a longas distâncias, objetivo das comunicações quânticas.

Em geral, o fóton não é um sistema de dois níveis, mas, se escolhermos apenas um grau de liberdade, teremos "artificialmente" criado um sistema destes a partir de um fóton e, desta forma, conseguimos utilizá-lo para codificar a informação quântica.

As formas mais usuais de uso do fóton para essa codificação são a polarização[4] e a fase (ou o "time-bin"). Já foi também utilizada experimentalmente a frequência [36] e ainda sugerida uma codificação em pares de pulsos consecutivos contendo, cada um, estados coerentes com 0 ou μ fótons ($\mu < 1$) e que possuem uma relação de fase entre si [37]. Para comunicações quânticas, ainda é possível utilizar o par posição-momento [38]. Pode-se facilmente utilizar fótons gerados por lasers atenuados (seção 3.2) para implementar estas codificações aqui citadas. Para este trabalho, estamos mais interessados na codificação em polarização.

Codificação em polarização

A polarização é uma escolha trivial para implementar qubits, uma vez que polarizações ortogonais são naturalmente sistemas de dois níveis e os lasers, fontes de fótons, são geradores de feixes de luz com polarização linear bem definida; é preciso apenas fazer com que o fóton passe através de componentes

[3] Assim como no caso de um qubit simples, não temos acesso direto à informação contida no estado final do registrador quântico. Os algoritmos de Shor e Grover são bons exemplos de algoritmos inteligentes o suficiente para tirar vantagem desse processo.

[4] Para uma breve explicação sobre a polarização da luz e formas de medi-la, consultar [35].

de birrefringência variável para que sua polarização seja variada. A associação entre a esfera de Bloch e a esfera de Poincaré de estados de polarização da luz é uma associação, pode-se dizer, de certa forma óbvia. Por exemplo, observando as duas esferas lado a lado, como na figura 3.2, a associação da base computacional ($|0\rangle$, $|1\rangle$) aos estados de polarização circular à direita e circular à esquerda ($|CD\rangle$ e $|CE\rangle$) é direta. Mas quaisquer pontos diametralmente opostos na esfera de Poincaré podem ser usados. A forma mais simples de realizar a codificação, até pelo fato da luz gerada por um laser ter polarização linear, é associar a base computacional às polarizações linear horizontal $|H\rangle$ e linear vertical $|V\rangle$ (ou $|\leftrightarrow\rangle$ e $|t\rangle$).

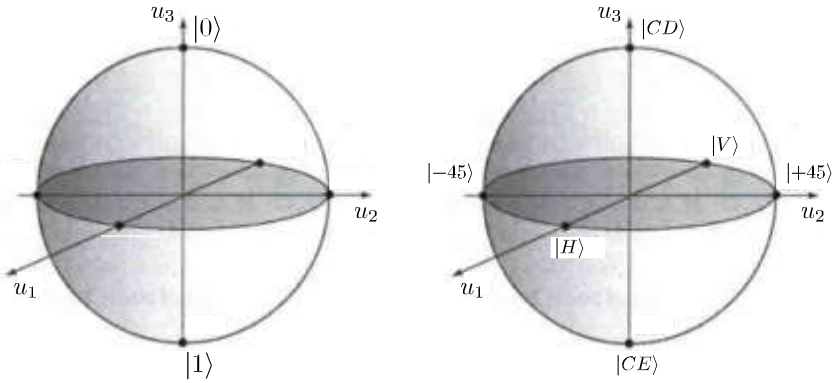


Figura 3.2: Representação dos qubits como pontos na superfície da esfera de Bloch, à esquerda, e representação dos estados de polarização na esfera de Poincaré, à direita.

Há ainda uma outra vantagem da codificação dos qubits em polarização. Caso deseje-se medir um qubit em uma base diferente da base computacional – por exemplo, na base de Hadamard (equação (3-4)) que corresponde aos estados de polarização lineares $|+45\rangle$ e $|-45\rangle$ – bastaria usar um componente semelhante na detecção.

O fóton sofre alteração em sua polarização ao atravessar um elemento birrefringente, que pode ser implementado de forma simples com uma lâmina de meia onda seguida de uma lâmina de quarto de onda, ambas com capacidade de giro sobre o mesmo eixo central, ou de forma mais eficiente para comunicações quânticas, com elementos eletro-ópticos, como os atuadores piezoelétricos. Para as demonstrações de que, de fato, o elemento birrefringente é capaz de gerar um estado de polarização arbitrário, ver [35].

Na figura 3.3 pode-se ver em (a) um esquema da preparação dos qubits e em (b) um esquema da forma de medir os qubits. No esquema de preparação, assume-se que os fótons na entrada estão em um estado de polarização conhecido. Os componentes U_i representam os elementos birrefringentes que

realizam transformação unitária (daí a notação U) no estado de polarização dos fótons.

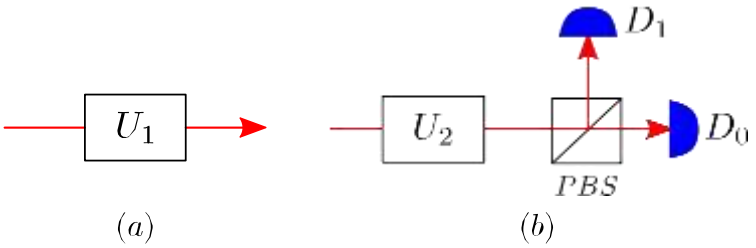


Figura 3.3: (a) Esquema para a preparação de qubits codificados em polarização e (b) esquema para a medida dos mesmos qubits.

Para a medição do estado de polarização, é colocado um separador de feixes polarizador (PBS), cuja função é "escolher" para qual caminho enviar o fóton: se o fóton em sua entrada possuir polarização vertical, ele é transmitido e detectado por D_0; no entanto, se sua polarização for horizontal, ele é refletido e detectado por D_1. Obviamente, se o fóton na entrada do PBS estiver em uma superposição de estados de polarização, ele poderá ir para qualquer uma das duas direções, com probabilidades que dependerão de seu estado de polarização, isto é, dependerão das amplitudes de probabilidade α e β.

3.2
Geração de Fótons Únicos por Lasers Atenuados

Atualmente, ainda não é possível obter uma fonte de fótons únicos perfeita, que seja capaz de gerar exatamente um fóton a cada ciclo, o que seria a fonte ideal. Como na teoria de comunicações quânticas dizemos que a informação é codificada em fótons únicos, precisamos criar uma forma de obter pulsos de luz contendo não mais que um fóton a cada ciclo (estado de Fock $|1\rangle$). Mas como fazê-lo?

Na prática, o que se faz é atenuar a saída de um laser até que o número médio de fótons por pulso seja tão pequeno que a probabilidade de haver mais de um fóton no mesmo pulso seja tão pequena quanto se queira. O consenso geral é que, para entrar em regime quântico, devemos trabalhar com um número médio de fótons por pulso $\mu \leq 0,1$.

Como os fótons produzidos por um laser não estão uniformemente espaçados no tempo, mas sim em um estado coerente, que é uma superposição dos estados de Fock, não teremos um fóton a cada pulso, mas sim probabilidades de zero ou um ou dois, etc fótons em cada pulso. Podemos calcular estas pobabilidades utilizando a representação da superposição dos estados de Fock:

$$|\mu) = e^{\frac{-\mu}{2}} \sum_n \frac{\sqrt{\mu^n}}{\sqrt{n!}} |n) \tag{3-7}$$

A distribuição de probabilidade $p(n)$ para a equação (3-7) é obtida fazendo-se $|(n|\mu)|^2$:

$$\begin{aligned} p(n) &= \left| (n| \; e^{\frac{-\mu}{2}} \sum_n \frac{\sqrt{\mu^n}}{\sqrt{n!}} |n) \right|^2 \\ &= \left| e^{\frac{-\mu}{2}} \sum_n \frac{\sqrt{\mu^n}}{\sqrt{n!}} (n|n) \right|^2 \\ &= \left| e^{\frac{-\mu}{2}} \frac{\sqrt{\mu^n}}{\sqrt{n!}} \right|^2 \\ &= \frac{\mu^n}{n!} e^{-\mu} \end{aligned} \tag{3-8}$$

Consideremos agora um laser *quasi-monocromático* cuja potência P da luz emitida seja constante. O fluxo médio de fótons é dado por $\Phi = \frac{P}{v}$ (*em fótons/s*), onde v é a frequência óptica. Em um intervalo de tempo τ correspondente à duração de um pulso, podemos afirmar que aproximadamente $\alpha.\Phi.\tau$ fótons foram capazes de passar pelo atenuador, cujo coeficiente de transmissão é α. Se dividirmos o intervalo de tempo τ em N sub-intervalos de comprimento τ/N, de forma que não haja mais de um fóton em qualquer sub-intervalo, cada sub-intervalo terá uma probabilidade $p = \alpha.\Phi.\tau/N$ de possuir um fóton e probabilidade $1 - p$ de estar vazio. A probabilidade de se encontrar n fótons distribuídos pelos N intervalos é dada por uma distribuição binomial descrita por:

$$\begin{aligned} p(n) &= \binom{N}{n} p^n (1-p)^{N-n} \\ &= \frac{(\alpha\Phi\tau)^n}{n!} \; \frac{N!}{(N-n)!N^n} \left(1 - \frac{\alpha\Phi\tau}{N}\right)^{N-n} \end{aligned} \tag{3-9}$$

Quando $N \to \infty$, o último termo tende a $e^{-\alpha\Phi\tau}$ e o penúltimo termo tende a 1. Como $\alpha\Phi\tau$ é o número médio de fótons por intervalo, $\alpha\Phi\tau = \mu$, e, portanto:

$$p(n) = \frac{\mu^n}{n!} e^{-\mu} \tag{3-10}$$

Note que o resultado da distribuição de probabilidade para a luz do laser (equação (3-10)) é exatamente o mesmo que para a superposição dos estados

de Fock (equação (3-8)). Esta é uma distribuição de probabilidade poissoniana e, por esta razão, não é possível obter uma quantidade indefinida de pulsos consecutivos que contenham exatamente um fóton. A distribuição poissoniana não é a ideal, pois a probabilidade dos pulsos com mais fótons decai muito lentamente, mas para uso em QKD isso não é um problema, pois pode-se conseguir um limite superior para a taxa de erro.

Por motivos que se tornarão claros na seção 3.5 sob o contexto de criptografia quântica, não é desejável a geração de pulsos contendo mais de um fóton. Observe que a probabilidade de um pulso não-vazio possuir mais de um fóton é dada por:

$$\begin{aligned} P(n>1 \mid n>0) &= \frac{1-p(0)-p(1)}{1-p(0)} \\ &= \frac{1-e^{-\mu}(1+\mu)}{1-e^{-\mu}} \\ &\approx \frac{\mu}{2} \end{aligned} \tag{3-11}$$

Percebe-se que é possivel tornar a probabilidade dos pulsos possuírem mais de um fóton tão baixa quanto se queira, bastando para isso diminuir o número médio de fótons por pulso. Por outro lado, há um *trade-off* entre esta probabilidade e a probabilidade de ser emitido um pulso vazio, que é dada por $p(0) = e^{-\mu} \approx 1-\mu$. Ou seja, quando μ é muito pequeno para que seja pequena a probabilidade de serem emitidos pulsos com mais de um fóton, aumenta a probabilidade de serem emitidos pulsos vazios, sem nenhum fóton, o que reduz a taxa de transmissão do sistema. Por exemplo, para $\mu = 0,1$, que é o limiar historicamente convencionado para o regime quântico:

$$\begin{aligned} p(0) &\approx 0,9\ (90\%) \\ P(n>1 \mid n>0) &\approx 0,05\ (5\%) \end{aligned}$$

Se quisermos reduzir a probabilidade de serem emitidos pulsos com mais de um fóton para 2,5%, teremos 95% de pulsos vazios, reduzindo ainda mais a taxa de transmissão.

O problema da redução da taxa de transmissão, a princípio, poderia ser eliminado se a freqüência de transmissão fosse aumentada – de MHz para GHz, por exemplo – mas o ruído na detecção não se altera e, assim, a relação sinal-ruído diminui.

Uma forma engenhosa de evitar o efeito negativo causado pelo aumento

da probabilidade de emissão de pulsos vazios, como, por exemplo, a proposta por Hong e Mandel [39], envolve o uso de um cristal não-linear. No esquema proposto, um laser de bombeio incide sobre um cristal não- linear de segunda ordem de forma a gerar pares de fótons pelo processo de *spontaneous parametric down-conversion*, que é um processo muito utilizado para a geração de pares de fótons emaranhados. Sendo a frequência do laser de bombeio v_p, a existência de um fóton de sinal gerado no cristal com frequência v_s implica na existência de outro fóton criado ao mesmo tempo, de frequência v_i (*idler*), tal que $v_s + v_i = v_p$. Portanto, o fóton em v_i pode servir de "testemunho" para a existência do fóton que está sendo enviado, na frequência v_s. Assim, se o transmissor detectar o fóton *idler*, ele pode informar ao receptor via canal clássico em quais momentos um fóton realmente foi enviado.

Para este esquema funcionar, dois processos precisam ter eficiências altas: primeiro, a geração no processo não-linear, que, infelizmente, em geral não passa de 10^{-6}, e, segundo, o detector utilizado para monitorar os fótons *idler*, pois, do contrário, apenas uma pequena fração dos pulsos contendo fótons será anunciada.

Há ainda um outro ponto digno de nota: esse esquema **não** soluciona o problema de pulsos multi-fóton, pois o laser utilizado para bombeio do cristal não-linear precisa ser muito intenso, logo, existe uma probabilidade de que dois pares de fótons sejam criados ao mesmo tempo. Uma ideia desenvolvida para atacar o problema do ataque PNS foi proposta por Hwang [40], através dos chamados *decoy states* ("estados isca"). Nesse esquema, Alice intencionalmente produz pulsos multi-fóton e os mistura aleatoriamente aos pulsos enviados a Bob. Após a transmissão, durante o processo de concicliação de base, eles verificam se houve perdas anormais para esse tipo de pulso. Se as perdas nos *decoy states* forem maiores que nos demais estados "normais", o protocolo é interrompido e a chave descartada. Desta forma, o sistema QKD que usa o esquema de *decoy states* não precisa necessariamente utilizar $\mu = 0,1$ fótons por pulso.

3.3 Canal Quântico

O canal quântico não é exatamente uma entidade diferente do canal clássico. Eles são exatamente o mesmo espaço físico, mas, quando a informação trafegando no canal é codificada em entidades quânticas, usualmente o chamamos de canal quântico. Além do mais, em comunicações quânticas, geralmente também há comunicação clássica ocorrendo ao mesmo tempo entre o transmissor e o receptor. Exemplos desse caso são a criptografia quântica e o

teletransporte quântico. Mas, do ponto de vista dos efeitos causados pelo meio na informação, ou mais precisamente, nas entidades portadoras de informação, entre o transmissor e o receptor, os canais quântico e clássico são muito diferentes e, portanto, a caracterização do canal se dá de forma bem distinta.

O efeito de atenuação é um exemplo de fácil entendimento para a compreensão dessas diferenças. Em qualquer canal real, o sinal está sujeito a sofrer atenuação, que é a perda de parte de sua energia para o meio, por vários fatores; entretanto, enquanto se fala sobre "pulsos atenuados" em comunicações clássicas, que podem resultar em uma decisão equivocada por parte do receptor sobre qual bit foi transmitido, não podemos falar em "fótons atenuados" no contexto de comunicações quânticas. O fóton não pode ser parcialmente atenuado. Ou ele chega ao receptor, ou não chega – por definição, não há opção intermediária nesse sentido. Assim como muitos conceitos em física quântica, a atenuação surge como um efeito estatístico que só pode ser verificado quando o mesmo experimento é realizado várias vezes, isto é, ela retrata a probabilidade de um fóton conseguir atravessar o canal sem ser destruído.

Na prática, o canal quântico poderia consistir em qualquer meio em que a luz possa se propagar, mas as escolhas mais apropriadas são as mesmas dos sistemas de comunicações ópticas clássicos: as fibras ópticas e a atmosfera. Intuitivamente, pensaríamos que fibras ópticas são mais próximas do ideal de "sistema fechado", no qual o ambiente não tem interação com o sistema, pelo fato de o sinal se encontrar espacialmente confinado, enquanto a atmosfera é aparentemente mais "aberta" a influências externas. Entretanto, essa intuição é equivocada. Alguns tipos de fibra, chamadas de fibras multimodo, admitem a propagação de vários modos espaciais do sinal luminoso ao mesmo tempo, que se acoplam facilmente entre si e, assim, atuam no qubit como um ambiente não-isolado. No entanto, para fibras monomodo, a intuição está correta, pois elas guiam apenas um modo de luz e por isso são muito apropriadas como canal quântico.

Em sistemas abertos, que é o caso deste trabalho, são dois os tipos *macro* de efeitos do ambiente sobre o sistema quântico que possuem análogo em sistemas clássicos: *ruído*, que é a "perda" de um fóton do ambiente para o sistema, e *atenuação*, que é a perda de um fóton do sistema para o ambiente.

Enquanto o ruído é uma inserção de informação espúria no sistema e causará, no máximo, uma confusão no receptor ao receber um fóton que não veio do transmissor, certos tipos de atenuação podem ser encarados como um "vazamento" de informação do sistema para o ambiente e, portanto, uma medida realizada no ambiente pode revelar propriedades do qubit original, o que, do ponto de vista da criptografia quântica, por exemplo, é certamente

indesejável.

Há, ainda, em um canal quântico, um tipo de perturbação sem análogo nos sistemas de comunicação clássica, chamado de *descoerência*, no qual há perda de informação (isto é, perda da fase relativa entre elementos de uma base para o qubit) sem que haja perda de energia.

3.4
Detecção de Fótons Únicos

A existência de (pseudo) fontes de fótons únicos e de canais através dos quais a informação quântica pode ser transmitida de nada adiantariam se não houvesse meios de detectar pulsos de luz contendo apenas um fóton. Neste trabalho, os detectores de fótons únicos utilizados são do tipo Detector de Fótons Únicos por Avalanche (SPAD), que, além do mais, são os detectores mais largamente utilizados em aplicações práticas. Foram utilizados os de *InGaAs* (arseneto de índio-gálio), utilizados para contagem de fótons no comprimento de onda de telecomunicações 1,55μm.

O SPAD, simplificando para entendimento, é um fotodiodo avalanche polarizado próximo ao ponto de avalanche. Ao detectar um ou mais fótons, ganha energia suficiente para entrar no modo avalanche e indica uma detecção. Note que, se incidirem no detector dois ou mais fótons dentro da mesma janela de detecção, o fotodiodo entrará em modo avalanche somente uma vez e, portanto, indicará apenas uma detecção para aquela janela. Ele não é capaz de identificar quantos fótons chegaram em uma mesma janela, mas apenas identificar se chegou energia (fóton) ou não.

As propriedades dos detectores que são relevantes no problema de contagem de fótons são *eficiência quântica*, *probabilidade de ruído*, *resolução temporal* e *tempo morto*.

3.4.1
Eficiência Quântica

A eficiência quântica de um contador de fótons é definida como a probabilidade de que um fóton incidente gere um pulso elétrico. No caso dos SPAD, essa eficiência é um produto de três eficiências primárias: em primeiro lugar, o fóton deve atingir a região fotosensível do detector; em seguida, deve ser absorvido, de forma a gerar um par elétron-buraco e, por último, esse par elétron-buraco deve ser capaz de iniciar uma avalanche.

A eficiência de detectores de *InGaAs*, na prática, dificilmente ultrapassa os 40%, ainda que idealmente quiséssemos uma eficiência de 100%. O efeito de uma baixa eficiência quântica é exatamente o mesmo efeito causado por perdas

(atenuação) no canal, e pode tornar um sistema de comunicações quânticas inviável, mesmo que a relação sinal-ruído seja boa.

Na realidade, cada material (seja semicondutor, supercondutor, etc) possui um tipo de dependência distinto com o comprimento de onda, sendo alguns mais sensíveis para certas regiões do espectro do que outros; portanto, a escolha do comprimento de onda de um sistema de comunicações quânticas vai depender essencialmente dos contadores de fótons disponíveis no mercado. De forma não muito surpreendente, para comunicações quânticas, são utilizados os mesmos comprimentos de onda dos sistemas de comunicações clássicos, afinal, já existe toda uma tecnologia disponível que pode ser imediatamente aproveitada. Valores muito comuns são 780 *nm*, 850 *nm*, 1300 *nm* e 1550 *nm*.

3.4.2 Probabilidade de Ruído

A probabilidade de ruído é definida como a probabilidade de um sinal elétrico ser gerado espontaneamente, independentemente da presença de fótons. Existem basicamente dois tipos de ruídos inerentes ao próprio detector: *ruído de escuro* e *afterpulses*. O ruído de escuro surge do fato de que pares elétron-buraco podem ser gerados por mecanismos outros que a absorção de um fóton, tais como processos de tunelamento entre as bandas de condução e valência ou, na maior parte dos casos, processos oriundos de agitação térmica. Isto ocorre pelo fato do fotodiodo do SPAD estar polarizado próximo à avalanche e, portanto, estas oscilações elétricas de geração de pares elétron-buraco podem levá-lo a entrar na região de avalanche. Ele é chamado de *ruído de escuro* porque ocorre mesmo sem luz incidindo no detector, e os pulsos elétricos gerados por este mecanismo são chamados de *contagens de escuro* (*dark counts*).

O *ruído de escuro* é um processo sem memória e pode ser modelado por uma variável aleatória poissoniana, da mesma forma que a geração de fótons por um laser atenuado. Analogamente ao fluxo de fótons (Φ) do caso de lasers atenuados, temos o termo chamado de taxa de escuro (n_{dark}), que expressa o valor médio de contagens por unidade de tempo. Todavia, a cada janela temporal de detecção o SPAD só gera, no máximo, um pulso de contagem, independente da quantidade de "fótons incidentes", sejam eles fótons reais ou ruído de escuro. Desta forma, não faz sentido falar em $p(n)$, ou seja, na probabilidade de haver n contagens de escuro por pulso, pois todos os casos em que $n \neq 0$ produzem o mesmo efeito. Logo, a probabilidade de ruído por pulso é dada por:

$$P(ruído) = 1 - p(0) = 1 - e^{-\mu_r} \quad (3\text{-}12)$$

onde $\mu_r = n_{dark} T$ é o número médio de contagens por pulso. Na prática, a duração T dos pulsos é muito pequena, da ordem de nanosegundos, de forma que μ_r é muito pequeno e (3-12) pode ser aproximada por $P(ruído) \approx \mu_r$.

Já os *afterpulses* estão associados ao efeito de cargas presas em "armadilhas" (níveis energéticos no interior do gap) devido a avalanches anteriores. Com a permanência dessas cargas nestes níveis durante a abertura da próxima janela temporal de detecção, o SPAD "entende" que há uma nova detecção. Esse efeito pode ser reduzido aumentando-se o tempo morto – o que não é desejável, como veremos na seção 3.4.4 – ou aumentando-se a temperatura, o que aumentaria a taxa de ruído de escuro e, portanto, também é indesejável.

Se reduzíssemos o SPAD a temperaturas baixíssimas, poderíamos conseguir eliminar as contagens de escuro, mas aumentaríamos a taxa de *afterpulses*. Portanto, estamos diante de mais um *trade-off*, desta vez no receptor, e devemos buscar trabalhar em temperatura que minimize o efeito conjunto do ruído de escuro–*afterpulse*.

3.4.3
Resolução Temporal

A resolução temporal de um detector é a incerteza no intervalo de tempo entre a detecção de um fóton e a geração de um pulso elétrico. Qualquer detector semicondutor possui um certo tempo de resposta devido a efeitos de difusão ou à capacitância do fotodiodo, mas no caso específico do SPAD, há de se considerar o tempo que leva para ocorrer a construção da avalanche, que é um processo aleatório decorrente da aleatoriedade do processo de multiplicação por avalanche. É essencial que a resolução temporal seja suficientemente inferior à duração do pulso, de forma que o efeito de *jitter* seja desprezível.

3.4.4
Tempo Morto

No caso de um detector ideal, após a geração de um pulso elétrico referente à detecção, o detector retornaria imediatamente à condição inicial, ficando "pronto para o próximo pulso", e a duração do intervalo entre duas janelas de detecção dependeria apenas de quão rapidamente o laser no transmissor seria pulsado. Como era de se esperar, os detectores reais não funcionam assim. Após gerar um pulso elétrico, seja ele proveniente de uma detecção verdadeira ou de ruído, o detector não retorna imediatamente à condição inicial. Ele leva um tempo para se "recuperar" do último pulso elétrico gerado. Este

efeito é conseqüência da eletrônica utilizada e não apenas do fotodiodo em si, e a este tempo de recuperação damos o nome de *tempo morto*.

De forma geral, os SPAD são polarizados com tensões superiores à de ruptura (modo *Geiger*) e, assim, um único fóton sensibilizando o detector já é capaz de gerar uma avalanche, que é composta de milhares de pares elétron-buraco. Mas o detector deve ser capaz de interromper de alguma forma a avalanche, para que um novo fóton gere uma nova avalanche e esta possa ser interpretada como uma nova detecção. O processo de interrupção da corrente elétrica é chamado de *quenching*. Com a tecnologia hoje disponível, que utiliza uma eletrônica sofisticada para fazer uma detecção ativa da presença de avalanche (*active quenching*), o tempo morto dos SPAD comerciais é da ordem de grandeza de alguns nanosegundos, podendo, em grande parte dos casos, ser ajustado para valores maiores.

Em sistemas síncronos, os fótons chegam no receptor em intervalos de tempo conhecidos. Neste tipo de sistema, é possível aumentar a tensão para além do limiar de ruptura somente nos instantes de tempo nos quais é esperada a chegada de um pulso. Esse método (*gated mode*) permite tempos mortos da mesma ordem de grandeza que os obtidos por *active quenching*, com uma eletrônica mais simples, porém, às custas da implementação de um sistema de sincronismo.

3.5
Criptografia Quântica

Criptografia é a arte de transmitir informações de tal maneira que elas não possam ser entendidas por um oponente que venha a interceptá-las. A informação original, chamada *texto claro*, consiste em palavras ou expressões retiradas de um vocabulário finito e reunidas de acordo com regras sintáticas definidas. A criptografia é um mapeamento determinístico inversível, produzindo um *texto cifrado* que não está de acordo com nenhuma dessas regras e parece aleatório e sem sentido, para que possa ser transmitido com segurança por um canal de comunicação público [41].

Nos dias de hoje, a criptografia se tornou uma necessidade básica. Virtualmente todas as transações financeiras e comerciais da atualidade dependem, de alguma forma, de poderosos algoritmos de criptografia, sem os quais o mundo definitivamente não seria o mesmo. Ao realizar qualquer transação bancária utilizando o *internet banking* ou realizar qualquer compra pela internet usando o cartão de crédito, estamos confiando na segurança que nos é dada por esses algoritmos.

Os sistemas de criptografia utilizados na maioria das aplicações comer-

ciais são os chamados *sistemas de chave pública* ou *sistemas assimétricos*, nos quais a segurança é baseada em complexidade computacional, entendida por complexa uma operação "difícil" para a qual seriam necessários métodos de força bruta que, com o poder computacional existente hoje em dia, poderia levar anos ou mesmo décadas para ser realizada. Um bom exemplo, que já foi citado *en passant* no início deste capítulo e que é largamente utilizado em protocolos de criptografia, é o problema de fatoração de números muito grandes, como por exemplo fatorar um número de 617 dígitos em seus dois fatores primos. Embora até os dias de hoje não exista nenhum método para realizar tais tarefas, elas não são fisicamente impossíveis de serem realizadas.

A solução para garantir a segurança da informação reside na utilização de sistemas de chave simétrica. Sistemas simétricos são aqueles nos quais uma mesma chave é utilizada nos processos de codificação (encriptação) e decodificação (decriptação). Uma analogia a esse sistema é um cofre no qual uma mensagem é trancada e o cofre enviado ao destinatário. Para recuperar a mensagem, o cofre deve ser aberto com a mesma chave com que foi trancado. Já foi demonstrado que existem sistemas simétricos incondicionalmente seguros, isto é, que não podem ser quebrados sem o conhecimento da chave.

Um método de criptografia comprovadamente seguro é a cifra de Vernam. O texto claro é escrito como sequência de bits (0 e 1). Outra sequência aleatória, chamada de chave é adicionada a ela, bit a bit, módulo 2. Essa adição é equivalente à operação booleana *XOR* (*OU exclusivo*). O texto cifrado resultante pode então ser descriptografado executando-se a operação *XOR* com a mesma chave. É essencial usar uma chave tão comprida quanto a mensagem e nunca mais usá-la. Quando a chave criptográfica da cifra de Vernam é usada somente uma vez, é chamada de *one-time pad*. Se a chave for verdadeiramente aleatória, nunca reutilizada e mantida em segredo, a cifra de uso único é imperscrutável. Também provou-se que toda cifra teórica inquebrável deve usar chaves com as mesmas exigências que chaves de *one-time pad*.

Se as partes envolvidas na comunicação compartilham o conhecimento da chave entre si e com ninguém mais, mensagens podem ser encriptadas e decriptadas de forma segura. Entretanto, este método é vulnerável à aquisição da chave por terceiros.

O problema que abordaremos nesta seção é como distribuir uma chave criptográfica (uma sequência secreta de bits) para vários participantes que inicialmente não compartilham de nenhuma informação secreta, usando um canal de comunicação intrinsecamente inseguro sujeito a interceptação por um espião. Se forem usados somente métodos clássicos, essa tarefa é impossível. Por outro lado, fenônemos quânticos nos provêm várias soluções. A criptografia

quântica é baseada na descrição fundamental da natureza, onde a segurança é garantida pela natureza das medições em física quântica, em oposição ao embasamento clássico de "dificuldade de execução".

A razão para esta diferença reside no fato que informação armazenada em uma forma clássica, por exemplo, texto impresso, imagem ou áudio, pode ser objetivamente examinada sem ser alterada em qualquer forma detectável, quanto mais ser destruída. Ao mesmo tempo, é impossível fazer isso a uma informação codificada em estados quânticos não-ortogonais desconhecidos, como a polarização de fótons. É a natureza escorregadia, enganosa, da informação quântica que a torna ideal para a transmissão de segredos.

Daqui por diante, daremos nomes aos participantes das transmissões criptografadas. Como normalmente é dito que deseja-se transmitir algo do ponto A para o ponto B, é recorrente nos textos que tratam de criptografia chamar o transmissor de Alice e o receptor de Bob, que desejam compartilhar uma chave secreta para trocar informações. Eva (derivado da palavra inglesa *eavesdropper* – aquele que se intromete, bisbilhoteiro) é uma espiã, ou simplesmente um elemento adverso, que quer obter o máximo de informação possível sobre a mensagem trocada por Alice e Bob. Em geral, assume-se que Eva tem total acesso ao canal de comunicações utilizado por Alice e Bob para transmitir a mensagem.

3.5.1
A Distribuição de Chaves

Como já foi dito anteriormente, Shannon demonstrou que se (a) a chave for verdadeiramente aleatória, (b) tiver o mesmo tamanho em bits que a mensagem e (c) nunca for reutilizada, então o one-time pad é perfeitamente seguro. O problema reside no fato de que tanto Alice quanto Bob devem ter conhecimento dessa chave, sem que Eva ou qualquer outro detenha esse conhecimento. Como, então, Alice poderia enviar a chave para Bob de forma segura, sem que Eva pudesse passivamente escutar o canal e obter informação sem ser detectada?

É exatamente aqui que entra a física quântica. A ideia da criptografia quântica é realizar a distribuição de chaves usando um sistema de comunicações quânticas. Note que o sistema de comunicações quânticas não é utilizado com o intuito de transmitir a mensagem propriamente dita. Por essa razão, a criptografia quântica é mais corretamente chamada de distribuição quântica de chaves (QKD, "quantum key distribution").

A ideia central por trás do QKD é que é impossível para um interceptador obter todas as informações do estado quântico transmitido. Mas o que

significa esta afirmação? Considere um único qubit no estado de superposição $|\Psi\rangle = \alpha|0\rangle + \beta|1\rangle$. Para uma única medição geral com α e β desconhecidos, é impossível determinar o estado $|\Psi\rangle$ com precisão. Por exemplo, se um "0" (zero) for obtido em uma única medição, é impossível determinar qual era o coeficiente α. Uma única medição indicando "0" não distingue entre $|0\rangle = |V\rangle$, $(|0\rangle + |1\rangle)/\sqrt{2} = |+45\rangle$ ou $(|0\rangle + i|1\rangle)/\sqrt{2} = |CD\rangle$, ou muitos outros estados possíveis na esfera de Poincaré. Em muitas e muitas medidas com cópias do estado é possível determinar o valor exato dele [42]. No entanto, no QKD, o qubit nunca é reutilizado e, portanto, é impossível para um espião determinar completamente o estado se vários estados não-ortogonais são usados. A chave para o QKD é o uso desses estados não-ortogonais.

Mas então, para obter informação sobre os bits que estão sendo transmitidos sem perturbar o sistema, Eva não poderia fazer várias cópias dos qubits enviados e medi-los até conseguir determinar os coeficientes α e β? O *teorema da não-clonagem* nos prova que não. Suponha que Alice codifique os bits em estados arbitrários distintos, da seguinte forma:

$$0 \rightarrow |\varphi\rangle, \qquad 1 \rightarrow |\phi\rangle \tag{3-13}$$

Os qubits $|\varphi\rangle$ e $|\phi\rangle$ formam uma base para o espaço de Hilbert H. Idealmente, a realização de cópias dos qubits poderia ser modelada como a aplicação de uma transformação unitária U que não perturbe os qubits sendo enviados, mas que, ao mesmo tempo, forneça informação a Eva. Neste contexto, Eva faz parte do "ambiente", aplicando uma transformação na qual o sistema principal (os qubits enviados) não sofre qualquer influência do ambiente. Dado que Alice transmite estados puros, podemos representar a transformação ideal a ser introduzida por Eva (a *máquina de clonagem*) como:

$$|\Psi^A\rangle \otimes |\Psi_0^E\rangle \longrightarrow^U |\Psi^A\rangle \otimes |\Psi^A\rangle \tag{3-14}$$

onde $|\Psi_0^E\rangle$ é o estado inicial do sistema usado por Eva, ou seja, o "ambiente". Se escrevermos a equação (3-14) substituindo o estado genérico enviado por Alice pelos dois estados $|\varphi\rangle$ e $|\phi\rangle$ obteremos o par de equações:

$$U\ |\varphi\rangle|\Psi_0^E\rangle = |\varphi\rangle|\varphi\rangle$$
$$U\ |\phi\rangle|\Psi_0^E\rangle = |\phi\rangle|\phi\rangle$$

Se fizermos o produto interno das equações, obtemos:

$$U^* U\langle\phi|\varphi\rangle\langle\Psi_0^E|\Psi_0^E\rangle = \langle\phi|\varphi\rangle\langle\phi|\varphi\rangle$$

$$\text{Ou seja, } \langle\phi|\varphi\rangle = \langle\phi|\varphi\rangle^2 \qquad (3\text{-}15)$$

Os dois lados da equação (3-15) são números complexos e a igualdade $x = x^2$ só possui solução se $x = 0$ ou $x = 1$. Portanto, o resultado dado pela equação (3-15) implica em $|\varphi\rangle = |\phi\rangle$ ou $|\varphi\rangle \perp |\phi\rangle$. Isto é, uma máquina de clonagem quântica só é capaz de fazer cópias dos qubits enviados por Alice se (a) todos forem iguais entre si (e neste caso não há informação transmitida) ou (b) os qubits forem codificados em estados ortogonais entre si. Mais uma vez, a chave para o QKD é o uso desses estados não-ortogonais.

Mas se é impossível distinguir estados não ortogonais, como Bob irá identificar os qubits enviados por Alice? Bob não terá meios de dizer, de forma determinística, se o qubit enviado por Alice foi um "0" ou um "1"! Será que, na tentativa de negar a Eva o conhecimento do conteúdo da mensagem, negamos também a Bob? Para que isso não aconteça, foram criados os *protocolos de criptografia quântica*. Os protocolos que compõem as bases da criptografia quântica são apresentados a seguir.

3.5.2
Os Protocolos BB84 e B92

3.5.2.1
Protocolo BB84

Em 1984, Charles Bennett e Gilles Brassard propuseram, em uma conferência da IEEE na Índia, o primeiro protocolo para criptografia quântica [8], que ficou conhecido pelas iniciais de seus nomes aglutinadas ao ano de sua proposição: BB84.

O protocolo consiste no uso de duas bases não-ortogonais entre si ($|u_1\rangle \perp |u_2\rangle$) e ($|v_1\rangle \perp |v_2\rangle$) e que sejam maximamente conjugadas ($|\langle v_i|u_j\rangle| = 1/\sqrt{2}$). Duas bases fáceis de implementar e que atendem a estes critérios são as bases ($|V\rangle, |H\rangle$) e ($|+45\rangle, |-45\rangle$). Os bits "0" e "1" são codificados nas duas bases. Tradicionalmente:

$$0 \rightarrow |V\rangle \text{ e } |+45\rangle$$
$$1 \rightarrow |H\rangle \text{ e } |-45\rangle$$

Além da sequência de bits a serem enviados ser uma sequência aleatória, como demandado pela cifra de Vernam, a escolha entre as bases para cada bit também deverá ser aleatória. Desta forma, Alice fará duas escolhas aleatórias para cada bit a ser enviado: qual bit deverá ser enviado ("0" ou "1") e qual base será usada para codificá-lo. Estatisticamente, Alice enviará cada bit

("0" ou "1") em 50% das vezes, utilizando cada base também em 50% das vezes, fazendo com que os quatro estados ($|V\rangle$, $|H\rangle$, $|+45\rangle$, $|-45\rangle$) sejam enviados com a mesma probabilidade de 25% cada. Assumindo inicialmente, por simplicidade, que o canal quântico utilizado não introduz ruído, Bob receberá todos os bits enviados por Alice, mas sem saber em qual base eles foram preparados. Então, como medi-los? Vimos na seção 3.5.1 que se Bob medir o qubit em uma base diferente da utilizada por Alice para sua preparação, ele não conseguirá obter informação determinística sobre o estado original do qubit. Por exemplo: se Bob medir um qubit na base $|V\rangle$, $|H\rangle$ e obtiver o resultado "0", ele não consegue determinar se o estado do qubit era $|V\rangle$, $|+45\rangle$ *ou* $|-45\rangle$. E o estado $|-45\rangle$ representa o bit "1"! Ou seja, sempre que Bob escolher a mesma base com a qual Alice codificou o qubit, ele obterá o mesmo bit que foi codificado por Alice; no entanto, se a base "errada" for escolhida, existe uma probabilidade de 50% de a medida resultar em um erro. Portanto, 25% dos bits recebidos por Bob conterão erros, uma taxa alta demais para qualquer tipo de comunicação.

Não há solução para isso. Alice não pode enviar de forma segura para Bob a informação sobre quais bases foram utilizadas em cada codificação antes que Bob realize as medidas para que ele consiga sempre medir na base "certa". Mas este fato é previsto no protocolo BB84 e, então, Bob terá que escolher também de forma aleatória qual base irá utilizar em cada medida realizada.

Ao final da transmissão, Alice e Bob iniciam a fase de conciliação de bases, em que anunciam as bases que cada um utilizou, através de um canal clássico público[5], como radiodifusão, por exemplo, e mantêm os bits que foram preparados/medidos na mesma base, descartando os bits em que foram utilizadas bases diferentes. É importante ressaltar que ambos anunciam apenas as bases utilizadas e não os resultados das medidas. Ao final da conciliação de bases, Alice e Bob têm uma subsequência de bits 50% menor que a sequência transmitida, mas, agora, as subsequências de Alice e de Bob são idênticas. Temos, então, *uma* chave. A figura 3.4 mostra um exemplo de comunicação utilizando o protocolo BB84, em que há ruído introduzido pelo canal quântico que impede Bob de obter medidas em dois qubits (quarto e décimo).

De qualquer forma, temos a impressão de que a informação das bases utilizadas poderia ser útil para Eva, e de fato pode ser. Visto que Eva não pode realizar cópias perfeitas dos qubits, de acordo com o teorema da não-clonagem, ela pode partir para uma estratégia diferente. Um exemplo simples de estratégia de espionagem é o chamado *método da interceptação-reenvio*, em

[5] É importante ressaltar que o canal clássico usado para reconciliação de bases seja *público*, ou seja, que possa ser monitorado por qualquer um mas impeça qualquer tipo de modificação na informação transmitida por ele.

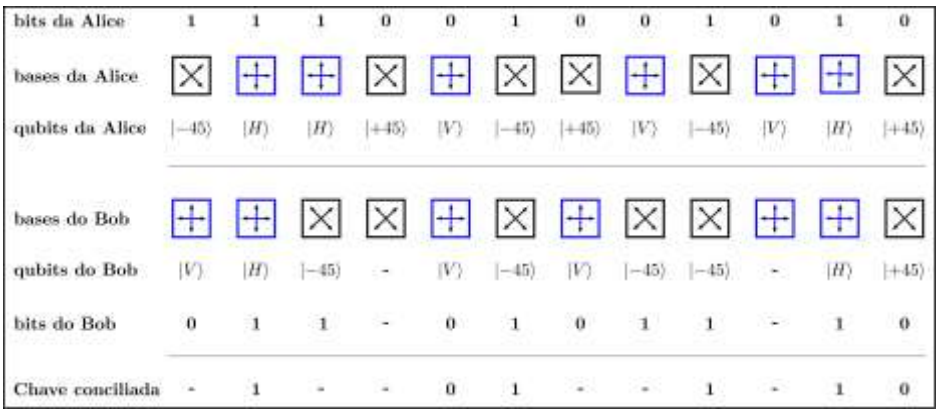


Figura 3.4: Representação de um QKD utilizando o protocolo BB84. Neste exemplo, Bob não obteve medidas para o quarto bit e para o décimo bit, devido a ruídos introduzidos pelo canal.

que Eva tentará realizar uma medida nos qubits transmitidos e preparar um qubit no mesmo estado em que ela mediu para enviar a Bob, se fazendo passar por Alice.

Eva não sabe qual estado foi enviado e, portanto, deve escolher se deseja fazer a medição na base ($|V\rangle$,$|H\rangle$) ou na base ($|+45\rangle$,$|-45\rangle$). Se Eva adivinhar a base correta (e ela não saberá disso até que Alice e Bob tenham se comunicado pelo canal clássico), ela poderá transmitir o estado correto a Bob (para que ele não saiba que foi interceptado). Se, no entanto, Eva escolher a base errada para medir, então o estado que ela transmite está errado e não é o que Bob deveria obter. Se Bob executar alguma forma de verificação de erro, verá que o estado errado foi enviado e, portanto, que Eva está presente.

Após a conclusão da transmissão, Eva tem acesso à conciliação de bases realizada por Alice e Bob, uma vez que é feita em um canal público. A princípio, Eva tem informação sobre 50% dos bits, que correspondem aos casos em que Eva escolheu a mesma base de medida que Bob. Mas há também os outros 50%, correspondentes à probabilidade de Eva medir na base errada e, portanto, transmitir o estado errado a Bob. Assim, não haverá acordo entre todos os bits da chave compartilhada de Alice e Bob. Eles podem verificar se um espião esteve presente selecionando um subconjunto dos bits da chave e dizendo publicamente um ao outro o que são. Ao verificar a taxa de erro (casos em que seus bits discordam), eles podem detectar a presença do interceptador e descartar a chave estabelecida. Se essa taxa de erro não for muito alta, Alice e Bob podem utilizar os bits restantes para criar uma chave compartilhada.

É claro que Eva poderia realizar essa estratégia em apenas uma pequena fração dos bits, e introduzir erros menores, ou ainda fazer clones imperfeitos dos qubits transmitidos por Alice, de forma a possuir alguma correlação entre

sua sequência de bits e a sequência compartilhada por Alice e Bob. Para evitar que Eva ainda possua informação a respeito da chave final, alguns algoritmos clássicos de correção de erros e amplificação de privacidade são utilizados. No final, Alice e Bob compartilham sequências idênticas contendo $m < n/2$ bits, onde n é a quantidade de bits inicialmente transmitida por Alice. Essa chave é chamada de chave secreta compartilhada .

Assim, existem duas possibilidades: (a) se não houver perturbações ou houver perturbações não muito altas, as leis da física quântica nos garantem que ninguém teve acesso a essa chave ou pode-se aplicar algoritmos clássicos de correção de erros e amplificação de privacidade e, portanto, a chave é estabelecida com segurança; ou (b) se houver perturbações altas, Alice e Bob sabem que alguém obteve informação a respeito da chave e eles simplesmente a descartam. É importante destacar que não há qualquer informação contida nos qubits transmitidos de Alice para Bob e interceptados por Eva. Os bits codificados não representam qualquer coisa até que Alice e Bob decidam usá-los como chave criptográfica e, portanto, se Eva for detectada e a sequência de bits descartada, o que Eva tem é apenas lixo.

Não podemos nos esquecer, entretanto, que o canal quântico pode introduzir ruído e que nem sempre a presença de erros é devida a um espião. Além disso, uma série de imperfeições na implementação prática podem ser fontes de erro. Isso significa que, na prática, uma presença excessiva de erros pode comprometer o sucesso dos algoritmos de correção de erros e amplificação de privacidade.

3.5.2.2 Protocolo B92

O protocolo BB84 foi generalizado para o uso de outras bases e estados. Uma das mais conhecidas generalizações é o protocolo B92 [43], que usa apenas dois estados não-ortogonais em vez de quatro estados. Este protocolo funciona da seguinte forma:

1. Alice gera um bit clássico aleatório $a = 0$ ou $a = 1$;
2. Se $a = 0$, Alice o codifica no estado $|V)$, se $a = 1$, codifica no estado $|+45)$, e transmite para Bob[6];

[6] Note que ambos os estados $|V)$ e $|+45)$ representam o bit "0" na codificação tradicional do protocolo BB84 (ver seção 3.5.2.1), logo, se Bob obtiver uma medida de um desses dois estados, ele associará ao bit clássico "0".

3. Bob, então, gera também um bit aleatório $a^i = 0$ ou $a^i = 1$;

4. Se $a^i = 0$, Bob mede o qubit recebido na base $(|V\rangle, |H\rangle)$ e, se $a^i = 1$, mede na base $(|+45\rangle, |-45\rangle)$, obtendo $b = 0$ ou $b = 1$;

5. Resultados possíveis:

   – $a = 0;\ a^i = 0 \quad \rightarrow \quad b = 0$
   – $a = 0;\ a^i = 1 \quad \rightarrow \quad p(b = 0) = 50\%;\ p(b = 1) = 50\%$
   – $a = 1;\ a^i = 0 \quad \rightarrow \quad p(b = 0) = 50\%;\ p(b = 1) = 50\%$
   – $a = 1;\ a^i = 1 \quad \rightarrow \quad b = 0$

6. Bob anuncia para Alice o resultado de b em um canal público e eles guardam todos os bits a e a^i correspondentes às medidas $b = 1$, mantendo secretos os bits a e a^i, que são a chave de Alice e Bob;

7. Alice e Bob podem executar os mesmos procedimentos de verificação de erros para detecção de espião no canal e, caso a taxa de erro não seja muito alta, executam algoritmos de correção de erros e amplificação de privacidade e a chave é estabelecida com segurança.

Observe que, ao final da utilização deste protocolo, as chaves de Alice e Bob são anti-correlacionadas, isto é, a cada bit "0" na chave de Alice, corresponderá um bit "1" na chave de Bob, e vice-versa.

Há ainda mais uma observação a fazer. A simplificação do sistema obtida com o uso de apenas dois estados não-ortogonais tem um custo. Enquanto no protocolo BB84, estatisticamente, a chave conciliada aproveita 50% dos bits transmitidos, no protocolo B92 este aproveitamento é de apenas 25%, correspondentes a metade dos casos em que os bits a e a^i são opostos, o que, por sua vez, corresponde a metade dos casos totais. Isto significa que a taxa de transmissão de bits no B92 é metade da taxa de transmissão de bits do BB84.

3.5.3
Implementação Prática

Qualquer implementação prática de um sistema de criptografia quântica deve buscar maximizar duas quantidades, que podemos compreender perfeitamente bem usando apenas o bom senso: a *distância máxima* que Alice e Bob podem estar separados um do outro para que uma chave secreta possa ser gerada e a *taxa máxima* de bits secretos por segundo que pode ser obtida. Afinal, se o sistema só puder ser usado por indivíduos a poucos metros de distância, ele não é necessário. Os indivíduos podem simplesmente se encontrar no mesmo ambiente e conversar. Ao mesmo tempo, se a taxa de bits por segundo para

estabelecer uma chave secreta for muito lenta, um carro-forte contendo vários pen-drives ou DVDs com chaves secretas seria muito mais apropriado. E o que limita a distância máxima e a taxa de geração de bits secretos são os mesmos fatores dos sistemas de comunicação clássica, só que em versão quântica: *as perdas e o ruído*.

Perdas surgem por vários motivos; por exemplo, um fóton se propagando pela atmosfera pode ser absorvido por alguma molécula ou espalhado por uma partícula de aerossol ou simplesmente passar direto pelo detector devido a erros de alinhamento. É evidente que, quanto maior a distância, maior a probabilidade de um fóton não chegar a seu destino.

O ruído também pode surgir de várias fontes, como por exemplo (ainda no caso da propagação atmosférica) luz do sol refletida por objetos no entorno do link ou espalhada pela atmosfera que atinge o receptor, ou (de forma geral) contagens de escuro do detector.

Esses dois fatores agindo em conjunto podem limitar severamente o desempenho do protocolo BB84. Podemos criar, então, a chamada *taxa de erro de qubit* (QBER) com o intuito de medir esses dois efeitos ao mesmo tempo, ruído e perdas; e ela é de simples interpretação física. A QBER é de extrema importância em qualquer sistema prático de distribuição quântica de chaves e é discutido a seguir. Em seguida, mostramos qual a relação entre a QBER e a segurança de um sistema de criptografia quântica e de que forma seu desempenho é afetado.

3.5.3.1
Taxa de Erro de Qubit (QBER)

A QBER é definida como a razão entre a probabilidade de se obter uma contagem falsa e a probabilidade total de haver contagens, medida por pulso.

Sem perda de generalidade com relação à forma de implementação dos qubits, podemos considerar uma codificação em polarização de fótons, com um esquema de detecção do tipo da figura 3.3(b)[7]. Temos, então:

$$QBER \equiv \frac{p_{falso}}{p_{total}} = \frac{p_{opt}.p_{foton} + p_{noise}}{p_{foton} + 2p_{noise}} \qquad (3\text{-}16)$$

onde p_{foton} é a probabilidade de ser detectado um fóton real e pode ser reescrita na forma $p_{foton} = \mu.\eta_{link}.\eta_{det}$, onde os termos à direita significam, respectivamente, o número médio de fótons por pulso, o coeficiente de transmissão do enlace e a eficiência do detector.

[7] Este é exatamente o esquema que foi utilizado na implementação prática deste trabalho, como será mostrado na seção 4.6.

As probabilidades P_{opt} e p_{noise} representam as fontes de contagens falsas. A primeira consiste na probabilidade de um fóton ir parar no detector errado devido a um contraste imperfeito de polarização (no caso de codificação em polarização); a segunda é a probabilidade de ocorrência de contagens de escuro e/ou contagens devido a fótons provenientes de fontes de ruído externas (são aquelas contagens indicadas pelo detector sem a presença de um fóton proveniente do transmissor).

Observe que o termo p_{noise} surge no denominador multiplicado por um fator 2, devido ao fato de haver dois detectores contribuindo para a existência de contagens. No entanto, no numerador, o fator 2 desaparece pois o ruído só produz erros nos casos em que ocorre no detector "errado", isto é, na metade do tempo. Claramente, pela própria definição dada em (3-16), a QBER corresponde à fração de bits errados na chave compartilhada por Alice e Bob após o processo de conciliação.

Nos casos em que $p_{noise} \ll p_{fóton}$, podemos reescrever a definição (3-16) como:

$$QBER \cong p_{opt} + \frac{p_{noise}}{\mu.\eta_{link}.\eta_{det}} \equiv QBER_{opt} + QBER_{det} \qquad (3\text{-}17)$$

Ou seja, a QBER pode ser aproximadamente escrita como uma soma de duas componentes, separadas de acordo com suas origens: uma "óptica" e uma de "detecção". Observe que a equação (3-17) só é válida se o valor da QBER for de apenas alguns porcento. Isto é sempre verdade para a componente óptica, que raramente ultrapassa 1% em esquemas de polarização (e também no de time-bins), mas nem sempre pode ser assumido para a componente de detecção. Nesses casos, nos quais o ruído de detecção é predominante, a QBER óptica pode ser desprezada.

3.5.3.2 Critérios de Segurança

Vimos anteriormente que o protocolo BB84 é perfeitamente seguro na ausência total de ruído, mas ao mesmo tempo sabemos que esse cenário está muito longe da realidade. Agora que introduzimos uma forma de se medir o ruído (QBER), podemos discutir uma condição suficiente para a segurança da criptografia quântica em sistemas reais.

A idéia básica por trás de qualquer discussão sobre segurança está no fato de que Alice, Bob e Eva, em algum momento, fazem medidas em seus qubits. Após as medidas, cada um deles possui um conjunto de variáveis aleatórias, que chamaremos respectivamente de α, β e ε. Definimos, então, uma distribuição de probabilidade conjunta $P(\alpha, \beta, \varepsilon)$ e nos faremos a seguinte pergunta: quais

condições essa distribuição de probabilidade conjunta deve satisfazer de forma que Alice e Bob possam extrair uma chave secreta?

A solução a esta pergunta não é trivial. O valor tradicionalmente usado para o que é conhecido como o limite para "segurança incondicional", demonstrado para ataques coletivos infinitos ([44],[45]) é $QBER \leq 11\%$. Mas, foi demonstrado em 2005 por Kraus *et al.* ([46]) que esse limite pode ser ligeiramente aumentado para $QBER \approx 12,4\%$ se um certo pré-processamento for realizado antes da aplicação dos algoritmos de correção de erro e amplificação de privacidade. Usaremos o valor de 12% na próxima seção[8].

É importante deixar claro que a teoria aqui apresentada não leva em conta ataques que se aproveitam das imperfeições dos equipamentos reais, como, por exemplo, aqueles apresentados por Makarov *et al.* em [47], [48], [49] e [50].

3.5.3.3 Taxa de Geração de Chave

Uma figura de mérito importantíssima de um sistema de criptografia quântica e que pode ser calculada a partir da QBER é a taxa de geração de chave, que também chamamos de *taxa líquida*, R_{net}. Ela é dada por:

$$R_{net} = R_{conc} F[\boldsymbol{I}(\alpha, \beta); \boldsymbol{I}(\alpha, \varepsilon)] \tag{3-18}$$

O termo R_{conc} representa a taxa de geração de chave após o processo de conciliação de bases entre Alice e Bob, e pode ser escrita na forma:

$$R_{conc} = \frac{1}{2}\boldsymbol{f}.p_{\boldsymbol{f}oton} = \frac{1}{2}\boldsymbol{f}.\mu.\eta_{link}.\eta_{det} \tag{3-19}$$

onde $\boldsymbol{f}$ é a taxa de repetição do laser utilizado por Alice, em pulsos por segundo. A função F depende do algoritmo utilizado por Alice e Bob para correção de erros e amplificação de privacidade, que, intuitivamente, supomos ser uma função das informações mútuas relevantes $\boldsymbol{I}(\alpha, \beta)$. Reescrevendo a equação (3-18), temos:

$$R_{net} = \frac{1}{2}\boldsymbol{f}.\mu.\eta_{link}.\eta_{det} F[\boldsymbol{I}(\alpha, \beta); \boldsymbol{I}(\alpha, \varepsilon)] \tag{3-20}$$

Da equação (3-20) fica clara a dependência da taxa de geração de chave (R_{net}) com relação ao número médio de fótons por pulso (μ), às perdas no canal (η_{link}), à eficiência na detecção (η_{det}) e a quão rapidamente Alice modula seu laser ($\boldsymbol{f}$). Não fica evidente, entretanto, a dependência da taxa líquida com a QBER.

[8] Não faz parte do escopo deste trabalho provar este limite, mas apenas usá-lo como embasamento para a caracterização e avaliação do esquema experimental utilizado. Para detalhes e provas sobre os valores, ver as referências citadas no texto e suas referências.

Segundo Christandl [45], podemos escrever $I(\alpha, \beta) = 1 - h(QBER)$, onde h é a função entropia binária[9] e, então, percebemos que a função F tem dependência com a QBER e, portanto, R_{net} também tem.

Observe que o termo $F[I(\alpha, \beta); I(\alpha, \varepsilon)]$ depende não apenas dos algoritmos utilizados, como também da estratégia de espionagem utilizada por Eva, e que, portanto, não é possível fornecer uma expressão geral para a taxa de geração de chave.

3.5.3.4 Pulsos Multi-Fóton e o Ataque PNS

Se aumentarmos o número médio de fótons por pulso, de acordo com a equação (3-11) a probabilidade de pulsos multi-fóton também aumenta. A título de comparação, a figura 3.5 mostra a distribuição de Poisson para dois valores médios diferentes $\mu = 1$ e $\mu = 0,1$.

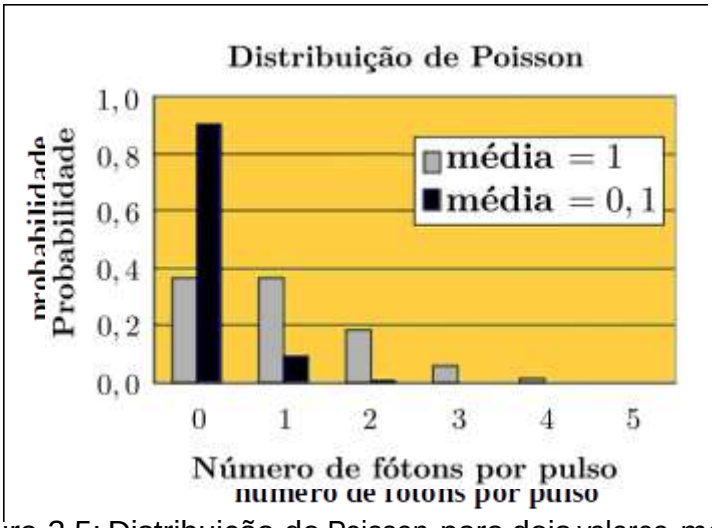


Figura 3.5: Distribuição de Poisson para dois valores médios de fótons por pulso.

Observando a figura, percebe-se que, com o aumento de μ, a probabilidade de pulsos vazios cai de 90% para menos de 40%. Todavia, a probabilidade de pulsos multi-fótons ($n \geq 2$), que era próxima de 0, ultrapassa os 20%. Não deve ser difícil, a essa altura, perceber por que um sistema de QKD não pode se dar ao luxo de pagar esse preço.

Suponhamos que Eva seja capaz de medir o número de fótons presentes em cada pulso sem introduzir nenhum distúrbio nos qubits e sem destruir nenhum fóton. Se a presença de mais de um fóton no mesmo pulso for detectada, Eva guarda um deles para si e permite que o restante siga na direção de Bob; caso contrário, ela bloqueia o pulso por completo. Em um pulso multi-fóton produzido por um laser, todos os fótons codificam a mesma informação.

[9] $h(c) = -c.\log_2(c) - (1-c).\log_2(1-c)$, onde c é a taxa média de erro.

Desta forma, Eva possui exatamente os mesmos qubits que Bob. Ao contrário do que ocorre no ataque de interceptação-reenvio, este ataque, chamado de *photon number splitting* (PNS), não introduz nenhuma espécie de distúrbio nos qubits recebidos por Bob, . Se Eva possuir uma "memória quântica", ela pode guardar seus fótons e postergar sua medida para o momento em que Alice anunciar quais bases usou para codificar seus qubits, de forma a obter informação sobre 100% da chave!

Pode-se argumentar que, a princípio, Alice e Bob poderiam detectar a presença de Eva devido à atenuação provocada pelo ataque PNS. Lembre que Eva bloqueia todos os pulsos de fótons únicos. Mas, para driblar esta possibilidade de ser detectada, bastaria que Eva utilizasse um outro canal, com menor atenuação, para transmitir os qubits dos pulsos multi-fóton a Bob, de forma que as perdas no ataque sejam compensadas. Apesar de a viabilidade técnica de tal ataque ser duvidosa, ela mostra claramente que a probabilidade de Alice gerar pulsos com dois ou mais fótons deve ser diminuída o quanto possível. Como mencionado anteriormente, o uso de $\mu = 0,1$ fótons por pulso não é essencial para QKD uma vez que seja usada a técnica de *decoy states*, como definido em [40], pois, com essa técnica, Alice e Bob conseguem detectar a presença de Eva no canal e, se for o caso, interromper o protocolo e descartar a chave.

3.5.4
Amplificação de Privacidade

Amplificação de privacidade é a arte de extrair informação compartilhada altamente secreta, talvez para uso como uma chave criptográfica, a partir de uma quantidade maior de informação compartilhada que é parcialmente secreta [51]. Suponhamos que Alice e Bob possuem uma variável aleatória X (uma sequência de n bits) e que Eva tem informação sobre parte dos bits de X, ou seja, uma variável aleatória correlacionada Y, tal que Eva possui no máximo $t < n$ bits de informação sobre X, isto é, $H(X/Y) \geq n - t$. Os detalhes sobre a distribuição P_{YX} são geralmente desconhecidos de Alice e Bob, exceto que satisfaz a limitação acima e talvez mais algumas.

O objetivo de Alice e Bob é, então, escolher uma função de compressão $g : \{0,1\}^n \rightarrow \{0,1\}^r$ tal que a informação parcial que Eva possuía sobre X e o conhecimento total de g façam com que ela tenha tão pouca informação sobre $S = g(X)$ quanto se queira. Eva terá total conhecimento sobre g porque sua escolha será comunicada via canal público. O S resultante é praticamente uniformemente distribuído, considerando toda a informação de Eva; portanto, pode ser usado com segurança como uma chave criptográfica.

O tamanho r da chave secreta que Alice e Bob podem extrair depende do tipo e da quantidade de informações disponíveis para Eva. Existem vários cenários possíveis a serem considerados. Eva pode obter (1) t bits arbitrários de X, (2) t verificações arbitrárias de paridade de X, (3) o resultado de uma função arbitrária mapeando cadeias de n bits para cadeias de t bits ou (4) a cadeia X transmitida através de um canal simétrico binário com probabilidade de erro de bit ε satisfazendo $h(\varepsilon) = 1 - t/n$ e, portanto, com a capacidade t/n, onde $h(.)$, mais uma vez, indica a função de entropia binária.

Para cada $s < (n - t)$, Alice e Bob podem extrair $r = n - t - s$ bits de chave secreta $S = G(X)$ enquanto mantendo a informação disponível para Eva sobre S exponencialmente pequena em s, escolhendo publicamente e de forma aleatória uma função de compressão G (que agora é uma variável aleatória) a partir de uma lista adequada de mapas em $\{0, 1\}^{n-t-s}$. Mais precisamente, Bennett [51] mostra que $H(S|G, Y = y) \geq r - 2^{-s}/(\ln 2)$, dado apenas que $R(X|Y = y) \geq n - t$. Ou seja, Eva sabe menos que $2^{-s}/(\ln 2)$ sobre S.

É claro que o comprimento r da chave secreta S que pode ser extraída por Alice e Bob depende de $P_{Y|X}$. De um modo mais geral, depende do tipo de restrição que $P_{Y|X}$ deve satisfazer. Quanto mais fortemente X e Y são correlacionados, menor é r. Da mesma forma, quanto mais restritiva for a estratégia disponível a Eva para selecionar $P_{Y|X}$, maior será r, em geral.

Tomemos um exemplo. Após a etapa de correção de erros, Alice e Bob compartilham, com alta probabilidade, uma chave reconciliada idêntica. Eles também conhecem a taxa de erro exata $\bar{E}$, que fornece uma estimativa muito boa da probabilidade de erro E. De forma conservadora, assumem que todos os erros foram causados por Eva. Eles também levam em consideração o vazamento durante a etapa de correção de erros, se houver. Então eles deduzem τ, o número de bits pelos quais a chave reconciliada deve ser reduzida para que as informações de Eva sobre a chave final sejam inferiores a um valor especificado, desejado. Mais precisamente, na maioria dos protocolos de distribuição de chaves quânticas, dado o inteiro τ, Alice escolhe aleatoriamente uma matriz binária K, $(n - \tau) \times n$, cujas entradas são 0 ou 1, e transmite K publicamente para Bob (sem criptografá-la). A chave secreta é, então:

$$k_{final} = K.k_{conciliada} \quad (mod 2) \tag{3-21}$$

A implementação da amplificação de privacidade é fácil, mas provar a segurança de todo o protocolo de distribuição de chaves quânticas é uma tarefa teórica difícil.

4
Desenvolvimento do Sistema de Comunicação

O capítulo descreve as etapas percorridas desde a definição dos objetivos experimentais deste trabalho até a escolha do setup experimental final a ser utilizado nos experimentos para estabelecer o enlace de comunicação óptica em espaço livre entre dois edifícios da universidade para transmissão de dados em regime quântico a uma distância de 160 metros, com a finalidade de estudar e analisar a possibilidade de serem estabelecidas chaves criptográficas secretas entre dois usuários através de QKD para uso em *one-time pad* e estudar a influência no enlace dos agentes externos, tais como luz do sol, névoa, chuva, vento e outros.

O projeto deve sempre contemplar um compromisso entre custo, disponibilidade de materiais, peso, dimensões e principalmente confiabilidade, com a definição teórica de uma linha geral de configuração do enlace e seu local de instalação. O local escolhido para a instalação do enlace foi a própria universidade, em dois locais onde já existiam suportes para a fixação dos canhões transceptores, bem como fácil acesso para transporte e instalação dos equipamentos necessários. Para o canhão transmissor, foi utilizado o telhado do Edifício Kennedy, acima do CETUC, a uma altura equivalente ao oitavo andar. Desta forma, foi possível manter o sistema transmissor dentro do laboratório de fotônica. O sinal óptico seria, assim, transmitido por uma fibra óptica interligando o sistema do laboratório ao canhão transmissor no telhado. Já o canhão receptor foi instalado em uma sacada no sexto andar do Edifício Cardeal Leme, a aproximadamente 160 metros de distância horizontal do transmissor, como pode ser visto na figura 4.1. Contígua à sacada, há uma sala com alimentação de energia elétrica e ar condicionado, o que possibilitou a instalação de todo o sistema receptor bem próximo ao canhão.

Para a execução deste trabalho, foi necessário desenvolver tanto o sistema de transmissão quanto o sistema de recepção, utilizando conhecimentos de opto-eletrônica, desde a escolha da forma de codificação dos bits clássicos “0” e “1”, passando pela seleção de várias possíveis formas de execução com diferentes equipamentos, até os testes em bancada para determinação do sistema que melhor atendesse ao objetivo proposto.

Figura 4.1: Local de instalação do enlace óptico. Imagem de Google Maps.

4.1 Seleção dos Equipamentos Básicos

Nesta seção são apresentados os equipamentos que formam a coluna mestra dos setups experimentais trabalhados, tendo cada um deles sido utilizado em todos os setups.

Acoplamento ao Meio de Transmissão e Captação do Sinal: Canhões Transceptores

A primeira premissa básica foi de serem utilizados o canhão transmissor e o canhão receptor desenvolvidos por Claiton Colvero para sua tese de doutoramento e que se encontravam disponíveis no laboratório[1]. O projeto, desenvolvimento e testes destes canhões foram realizados entre os anos de 2001 e 2005. Pela figura 4.2 é possível perceber o desgaste causado pelo tempo na estrutura dos canhões, que ficaram expostos ao tempo em seus locais de instalação por pelo menos catorze anos.

Devido à diferença entre o objetivo deste trabalho e o objetivo de Colvero, foi necessário realizar uma alteração no sistema de detecção da luz no canhão receptor, o que o tornou mais semelhante ao canhão transmissor. O objetivo de Colvero foi realizar "uma análise detalhada teórica e experimental da viabilidade destes sistemas de comunicações ópticas em diferentes condições

[1]Para detalhes sobre o processo de desenvolvimento dos canhões, características e testes, ver referência [26].

Figura 4.2: Acima, fotos dos canhões transceptores em seus invólucros (receptor à esquerda e transmissor à direita) e, abaixo, canhão transmissor sem a tampa do invólucro.

meteorológicas através da análise comparativa de três enlaces de diferentes janelas de propagação da atmosfera, sendo uma logo acima do visível, operando em 780 nm, uma no infravermelho próximo, no comprimento de onda comercial de 1550 nm e uma nova para esta aplicação situada no infravermelho distante, com comprimento de onda de 9100 nm [26]." Foi utilizada por ele potência óptica bem acima daquela para comunicação quântica, o que possibilitou a utilização de detectores ópticos padrão, em lugar dos detectores contadores de fótons utilizados neste trabalho. O receptor original tinha o detector óptico e o filtro da luz solar dentro do canhão, enquanto que, para este trabalho, foi necessário introduzir uma lente convergente e uma fibra óptica dentro do canhão, para acoplamento da energia óptica na fibra, ficando a filtragem e a detecção do sinal óptico situadas externas ao canhão. O principal motivo desta necessidade é a indisponibilidade de detectores contadores de fótons de tamanho físico reduzido que caibam dentro do canhão. Para fixação da fibra no lugar do detector original foi necessário projetar e fabricar uma nova peça de suporte em que se conectassem a fibra e a lente ocular para convergência do feixe na fibra. A peça, já com a fibra e a lente conectadas, pode ser vista na figura 4.3.

Após a alteração realizada no canhão receptor, os dois canhões passaram a apresentar as mesmas características básicas: em uma extremidade do canhão, uma fibra óptica multimodo, devido à maior abertura numérica se comparada à fibra monomodo, situada na frente de uma lente ocular

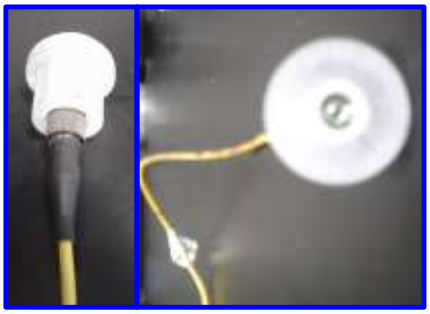


Figura 4.3: Fotos da nova peça projetada para o canhão receptor.

convergente, além de uma lente objetiva na outra extremidade do canhão, como pode ser observado no esquemático da figura 4.4.

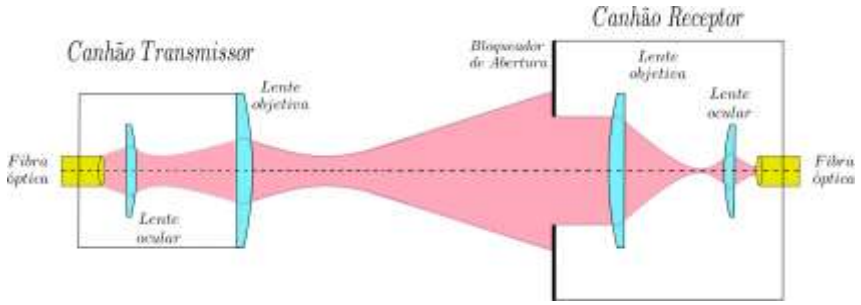


Figura 4.4: Esquemático (fora de escala) dos canhões de transmissão e de recepção, representando a transmissão de um feixe gaussiano.

Por estarem há catorze anos sem uso e terem ficado todo este tempo instalados em área aberta, sujeitos às intempéries, foi necessário, antes de tudo, verificar a integridade dos componentes dos canhões, realizar a limpeza e recuperação das partes móveis e dos componentes e substituir as fibras ópticas a eles conectadas, a fim de recuperar sua operabilidade.

Fonte Óptica: Seleção do Laser

A fonte óptica selecionada foi um laser de estado sólido, do tipo DFB[2], de onda contínua, emitindo no comprimento de onda de 1547,72 *nm*, com ajuste de potência variável entre $-10\ dBm$ e $+10,5\ dBm$ e largura de linha de $4\ MHz$. Este foi o laser selecionado devido à sua disponibilidade no laboratório, à existência de uma rede de Bragg casada em comprimento de onda com ele, o que facilita a filtragem de ruídos, e ao fato de seu comprimento de

[2]Para mais detalhes sobre o laser DFB, ver capítulo 15 da referência [27] e capítulo 3 da referência [1].

onda se encontrar dentro da região de transparência das lentes dos canhões transceptores a serem utilizados e da janela atmosférica de 1550 *nm*.

Modulação: Gerador de Funções Arbitrárias – AFG

Para gerar a sequência de bits clássicos, foi utilizado o gerador de funções arbitrárias (AFG)[3], com sequências de bits pseudo-aleatórias geradas em Python. O AFG não foi utilizado como modulador propriamente dito do sinal óptico, mas sim como seletor, ao gerar dois níveis de tensão representando os bits clássicos e aplicar estes níveis em algum tipo de equipamento óptico, cujo chaveamento da entrada modula o sinal óptico de saída. Um sinal elétrico equivalente a uma onda quadrada seria o suficiente para alternar os bits transmitidos entre os equivalentes aos clássicos 0 e 1. Entretanto, uma mensagem real não é composta de bits perfeitamente alternados e uma sequência para estabelecimento de uma chave secreta certamente também não é. Uma boa chave secreta é estabelecida a partir de uma sequência aleatória de bits. Tendo em vista a grande dificuldade de se criar uma sequência de bits perfeitamente aleatória, foi feito um código em Python utilizando a função *random* para criar várias sequências pseudo-aleatórias de 200 bits cada (limitação da entrada do AFG). Estas sequências foram utilizadas como entrada do AFG para geração do sinal. A cada fim de ciclo de 200 bits a sequência reinicia no primeiro, repetindo-se indefinidamente até que seja interrompida pelo usuário.

Filtragem: A Rede de Bragg

O objetivo do uso da rede de Bragg[4] é filtrar ruídos nos comprimentos de onda diferentes do comprimento de onda do laser, principalmente os provenientes da luz do sol. A rede reflete o comprimento de onda para o qual foi projetada, ao mesmo tempo em que transmite os outros comprimentos de onda. Pelo fato de estarmos interessados justamente na parte da energia que é refletida, é necessário utilizar um circulador óptico[5] antes da rede de Bragg, para direcionar o sinal desejado, refletido, para os detectores, enquanto os outros comprimentos de onda são transmitidos pela rede para fora do sistema. A largura do filtro é de 0,55 *nm*, conforme medido por testes em bancada

[3]Informações detalhadas sobre o Gerador de Funções Arbitrárias encontram-se em [52] e em [53].

[4]A teoria sobre o princípio de Bragg pode ser encontrada em [1].

[5]Um circulador óptico é um dispositivo que direciona a luz: a energia que entra pela porta *n* é direcionada somente para a porta *n* + 1, sem passar para as outras portas.

utilizando um laser de grande largura de linha, e o comprimento de onda filtrado, como mencionado anteriormente, é "casado" com o do laser, centrado em 1547,72 *nm*.

Detecção: Detector de Fótons Únicos por Avalanche – SPAD

Para trabalhar em regime quântico, faz-se necessário um detector capaz de realizar contagem de fótons, como o SPAD (detector de fótons únicos por avalanche, na sigla em inglês), utilizado neste trabalho.

Sua eficiência pode ser selecionada no menu do próprio detector, não passando de 25%. A seleção de eficiência nada mais é do que polarizar o fotodiodo mais próximo da avalanche (eficiência maior) ou menos próximo da avalanche (eficiência menor). O SPAD apresenta a chamada contagem de escuro, conforme explicado na seção 3.4.2. Como dito anteriormente, quanto maior a eficiência selecionada, mais próxima da avalanche está o fotodiodo e, portanto, mesmo pequenas oscilações são capazes de levá-lo à avalanche[6]. Assim sendo, quanto maior a eficiência selecionada, maior é a contagem de escuro. Com um *clock* de 1 MHz e eficiência de 25%, a contagem de escuro apresentada pelo SPAD é da ordem de 135 contagens por segundo, ou 135 Hz. Para um *clock* de 100 kHz e eficiência de 10%, a contagem de escuro apresentada pelo SPAD é da ordem de 10 contagens por segundo, ou 10 Hz.

Adicionalmente, foram feitas medições em bancada com todas as luzes do laboratório acesas e também apagadas, com e sem a rede de Bragg no circuito e foi comprovado que a energia das luzes do laboratório não apresenta influência alguma na detecção do SPAD.

Armazenamento e Interpretação dos Dados Recebidos

Associados ao SPAD, são necessários uma *Field Programmable Gate Array* (FPGA[7]) e um computador, para regular o *clock* do SPAD e extrair a informação sobre as detecções realizadas. O SPAD indica apenas quantas detecções por segundo foram realizadas, mas não indica o momento ou a sequência em que elas ocorreram. Entretanto, a cada detecção, seja ela real ou de escuro, o SPAD gera um pulso elétrico em uma de suas saídas, que foi conectada à FPGA. Como ela é quem gera o *clock* para o SPAD, cada pulso de detecção é associado a um momento específico relativo ao *clock* e, desta forma,

[6] Informações sobre funcionalidades e configurações do SPAD podem ser encontradas em [54].

[7] Foi utilizada uma FPGA integrada com controle da empresa Opal Kelly [55].

é obtida uma sequência de bits no receptor correlacionada à sequência de bits transmitida. O computador é utilizado para programar a FPGA e coletar, armazenar e interpretar os dados, que inicialmente são guardados em uma memória volátil pela FPGA. O código da FPGA foi desenvolvido em linguagem VHDL [56], enquanto sua interface gráfica no computador e o protocolo de comunicação entre os dois foram desenvolvidos em Python. Já a interpretação dos dados coletados pelo computador é feita em um código desenvolvido em MATLAB.

Equipamentos específicos de cada setup

Com a coluna mestra do sistema já selecionada, o passo seguinte foi o desenvolvimento e teste em bancada das funcionalidades de alguns setups experimentais, utilizando uma montagem *back-to-back* dos canhões, colocados a 1, 60 metros de distância entre suas lentes objetivas e diferentes equipamentos periféricos. Somente após a seleção do setup definitivo é que o sistema foi instalado ao ar livre, a 160 *m* de distância e sujeito às intempéries e variações climáticas. O desenvolvimento destes setups e uma breve explicação sobre eles são apresentados nas próximas seções.

4.2 Primeiro Setup: Modulação em Amplitude

O primeiro setup testado utilizou a codificação de bits clássicos em nível alto e nível baixo, como em uma comunicação clássica, modulando o laser em amplitude (AM), alterando sua intensidade através do uso de um interferômetro de Mach-Zehnder[8]. O esquemático deste setup é apresentado na figura 4.5, onde as linhas azuis representam fibras ópticas, com sinais ópticos, e as linhas pretas representam fios ou cabos elétricos, com sinais elétricos. Esta mesma representação de cores se repete em todos os esquemáticos apresentados ao longo deste trabalho.

Para a modulação em amplitude, o conceito utilizado é de se controlar a interferência da luz para realizar uma modulação em amplitude a partir da modulação em fase inserida pelo material eletroóptico (niobato de lítio[9] – $LiNbO_3$), ao colocar este material em apenas um dos caminhos de um interferômetro de Mach-Zehnder. Desta forma, por um dos caminhos passará diretamente a luz emitida pelo laser e pelo outro passará uma versão modulada em fase desta mesma luz. As duas versões desta luz interferirão na saída do

[8] Uma descrição de interferômetros pode ser estudada na seção 2.5 de [27].

[9] Existem várias fontes onde pode ser estudada modulação de fase utilizando o $LiNbO_3$. Uma delas é [57]. Sobre o material propriamente dito, $LiNbO_3$, pode–se consultar [58].

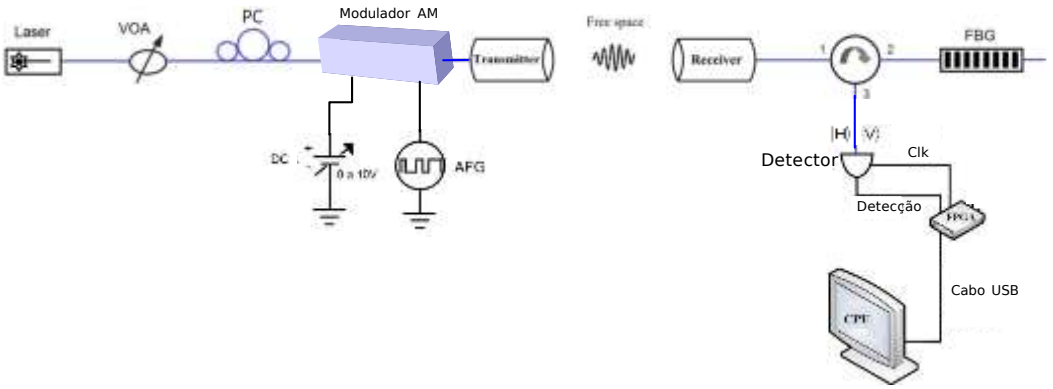


Figura 4.5: Primeiro setup experimental: modulação em amplitude.

Mach-Zehnder. A depender da fase inserida pelo $LiNbO_3$, esta interferência pode ser desde totalmente construtiva (atraso de fase múltiplo de 2π) até totalmente destrutiva (atraso de fase múltiplo de π). O atraso de fase é controlado através de tensão elétrica aplicada sobre o $LiNbO_3$, que altera o seu índice de refração, e, consequentemente, altera também o caminho óptico e, portanto, a fase da luz na saída do material. Se a amplitude desta tensão aplicada for variável, obtém-se uma modulação em fase da luz na saída do niobato de lítio que, ao interferir com a versão não modulada desta mesma luz, que passou pelo outro caminho do Mach-Zenhder, gera, na saída, a modulação em amplitude da luz que entrou no interferômetro. Como resultado, uma sequência de bits elétricos aplicada ao modulador produz uma réplica óptica desta sequência de bits. O modulador deve ser alimentado com uma tensão DC (*bias*) e uma AC (para modulação). Associado ao modulador, em sua entrada, foi conectado o controlador manual de polarização (PC), utilizado para maximizar sua saída, pois este é sensível à polarização da luz em sua entrada.

Para este trabalho, a tensão de *bias* aplicada foi a de quadratura, com o objetivo de modular a saída na região aproximadamente linear do modulador, a fim de obter uma relação direta simples entre o sinal de entrada e o de saída e, principalmente, de evitar a geração de harmônicos, o que ocorre quando a região não-linear é utilizada. Após experimentos no laboratório, foi determinado que o ponto de quadratura é em $3,6\ V$ e a região que pode ser aproximada por linear varia aproximadamente de $1,5\ V$ em torno da quadratura.

Para este primeiro setup, os bits clássicos foram codificados no AFG em $1,5\ V$ para o bit 1 e $0,0V$ para o bit 0 que, aplicada em conjunto com a tensão DC de $3,6\ V$, gera os bits ópticos a serem transmitidos: $bit\ 1 = 0,1\ mW$ de potência óptica e $bit\ 0 = 0,03\ mW$ de potência óptica,

para uma potência de entrada de $0,46\,mW$. Como a potência de saída varia linearmente com a potência de entrada, foi colocado um atenuador óptico variável (VOA) na saída do laser, para ajustar a potência de entrada no modulador e, consequentemente, a potência de saída no canhão e poder obter potência baixa o suficiente para entrar em regime quântico.

Trabalhando em regime quântico, com apenas um fóton representando cada bit transmitido, e com a eficiência do SPAD selecionada em seu máximo (25%) pelo menos 75% das janelas de detecção abertas não apresentarão qualquer detecção. Após os testes em bancada, este setup se mostrou altamente ineficiente para o objetivo deste trabalho, pois a codificação do bit 0 é confundida com a ausência de detecção e, desta forma, uma sequência pseudo-aleatória de bits transmitida, que deveria apresentar aproximadamente a mesma quantidade de bits 0 e 1 detectados, apresenta em torno de 87,5% de bits 0. Para exemplificar, caso a sequência transmitida fosse uma onda quadrada, deveríamos ter sempre a alternância entre bits de uma janela de *clock* de detecção para a próxima. Nosso sistema apresenta, em média, sete bits 0 para cada bit 1 detectado, devido à ausência de detecção ser interpretada como um bit 0 detectado. Este setup foi então descartado e um segundo setup foi desenvolvido.

4.3 Segundo Setup: Codificação em Polarização – Introdução da Chave Óptica

Com a impraticabilidade de trabalhar em regime quântico com a codificação dos bits clássicos em amplitude do sinal, tornou-se necessária uma nova forma de codificar os bits. A solução aplicada foi a codificação em polarização da luz. Uma determinada polarização representaria o bit clássico 0, enquanto a polarização ortogonal àquela representaria o bit clássico 1. O esquemático do setup desenvolvido pode ser visto na figura 4.6.

As polarizações utilizadas são aquelas alinhadas com os eixos do divisor de feixe polarizador[10] (PBS) utilizado no receptor, que é o responsável por separar os bits recebidos, transmitindo-os para cada canal de saída e, portanto para cada SPAD, de acordo com a polarização, que representa os bits. Devido à indisponibilidade temporária de polarímetro no laboratório, não foi possível medir quais são extamente estas polarizações, mas, de qualquer forma, esta informação não é relevante para este trabalho, uma vez que quaisquer polarizações ortogonais são suficientes para atingir o objetivo desejado, e isso, o PBS fornece, independentemente de qual seja. Para simplificação do raciocínio,

[10] Para o entendimento do funcionamento de um PBS, consultar a Seção 6.6 de [27].

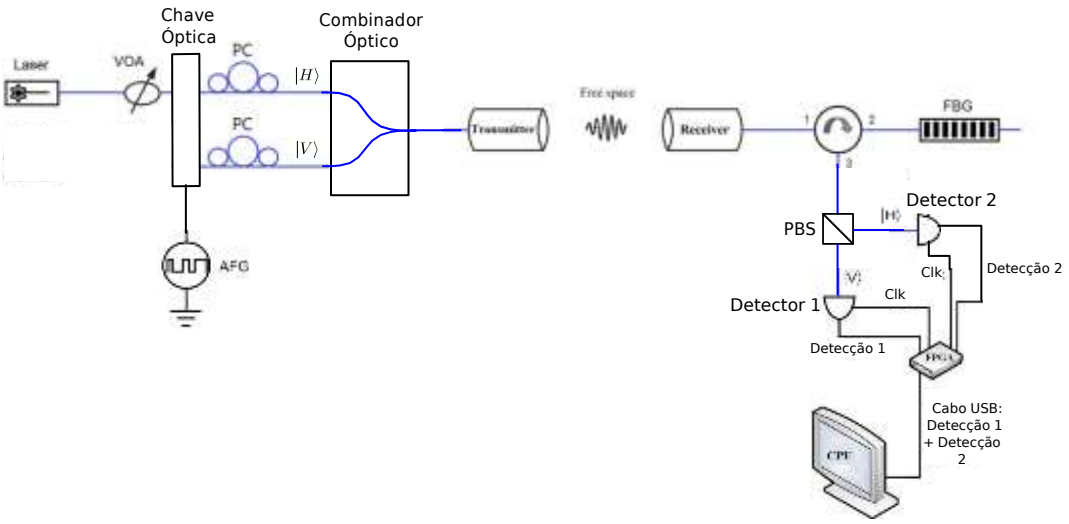


Figura 4.6: Segundo setup experimental: codificação em polarização, utilizando chave óptica para seleção dos bits.

assumiremos as polarizações mais simples de serem entendidas: bit clássico 0 codificado em polarização linear horizontal, $|H\rangle$, e bit clássico 1 codificado em polarização linear vertical, $|V\rangle$.

Uma chave óptica foi introduzida no sistema, com a função de selecionar um dentre dois caminhos possíveis para a luz do laser, atuando como um demultiplexador. O seletor da chave é controlado pelo AFG, cujas sequências pseudo-aleatórias gerarão uma sequência de níveis altos e baixos de tensão, selecionando, então, uma saída da chave (nível alto $= 3,5\,V$) ou a outra saída (nível baixo $= 0,0\,V$). Cada uma das duas saídas é ligada individualmente a controladores manuais de polarização (PC), onde são feitos ajustes prévios para obter em cada um dos caminhos uma polarização alinhada com um dos eixos do PBS do receptor. Desta forma, ao selecionar uma ou outra saída da chave óptica, está sendo selecionada uma ou outra polarização na entrada do combinador óptico e, portanto, na entrada do canhão transmissor. Assim sendo, o seletor da chave óptica determina qual bit clássico está sendo codificado e transmitido naquele momento. O atenuador óptico variável (VOA) na saída do laser foi mantido com a mesma função anteriormente descrita: ajustar a potência de entrada na chave óptica e, consequentemente, a potência de saída no canhão, e poder obter potência baixa o suficiente para entrar em regime quântico.

No receptor, faz-se necessário o acréscimo, além do PBS, de um SPAD adicional. Os fótons recebidos no canhão receptor, após a filtragem do ruído, serão destinados a uma das saídas do PBS, de acordo com a sua polarização. Desta forma, quando for transmitido um bit em $|H\rangle$, ele será detectado em um SPAD, que chamaremos de SPAD-0 e, quando for um bit em $|V\rangle$, será

detectado no outro SPAD, que chamaremos de SPAD-1.

Neste novo setup, o código desenvolvido em MATLAB para o receptor, que interpreta os dados recebidos pela FPGA oriundos dos dois SPAD, considera que foi recebido um bit 0 quando o SPAD-0 acusa uma detecção e o SPAD-1 não acusa e, inversamente, considera recebido um bit 1 quando o SPAD-1 acusa uma detecção e o SPAD-0 não acusa. Esta é a grande vantagem desta codificação dos bits quando comparada à modulação AM testada anteriormente. Não há confusão entre um dos bits e a ausência de detecção, uma vez que, se ambos os SPAD não acusarem detecção, a interpretação é de que não houve um bit detectado, mas sim uma janela de *clock* vazia, sem bit.

Existe ainda um quarto estado para este sistema, que ocorre quando os dois SPAD acusam detecção na mesma janela de detecção. Obviamente, um fóton não pode ter as duas polarizações ao mesmo tempo, portanto, ou um dos detectores está acusando contagem de escuro enquanto o outro detectou um fóton, ou os dois estão acusando contagem de escuro (ainda que isso seja muito menos provável). Neste caso, o código interpreta aquela janela como lixo detectado e o resultado é o mesmo da falta de detecção: não está associado a nenhum bit e temos uma janela de *clock* vazia, sem bit.

Este setup funcionou bem em bancada, demonstrando que a polarização dos fótons é uma escolha adequada para a codificação dos bits clássicos. Entretanto, ela apresenta duas dificuldades. A primeira é que o ajuste prévio das polarizações ortogonais se faz variando os PC manualmente no transmissor enquanto se observa a reação dos SPAD no receptor, o que é simples de ser feito na bancada, com transmissor e receptor em *back-to-back*, mas não na montagem entre dois edfícios. A segunda é que a chave óptica tem, na realidade, seleção mecânica e, portanto, muito lenta. Isto é, o sinal transmitido entre a entrada e uma das saídas é óptico, a escolha ou seleção de qual canal de saída será utilizado é feita por tensão elétrica, mas é uma movimentação mecânica de uma fibra óptica que efetivamente troca a saída em uso. Para tentar solucionar a primeira dificuldade, foi desenvolvido o terceiro setup experimental.

4.4
Terceiro Setup: Ajuste de Polarização no Receptor

A única modificação inserida neste setup foi um controlador manual de polarização (PC) no receptor, na entrada do PBS, como pode ser visto na figura 4.7. O ajuste de polarização é feito inicialmente substituindo a conexão com o canhão transmissor por uma conexão com um PBS adicional e fazendo a regulagem dos PC do transmissor para obter os estados ortogonais. Na

sequência, é feita a reconexão com o canhão transmissor, retirando do circuito o PBS adicional.

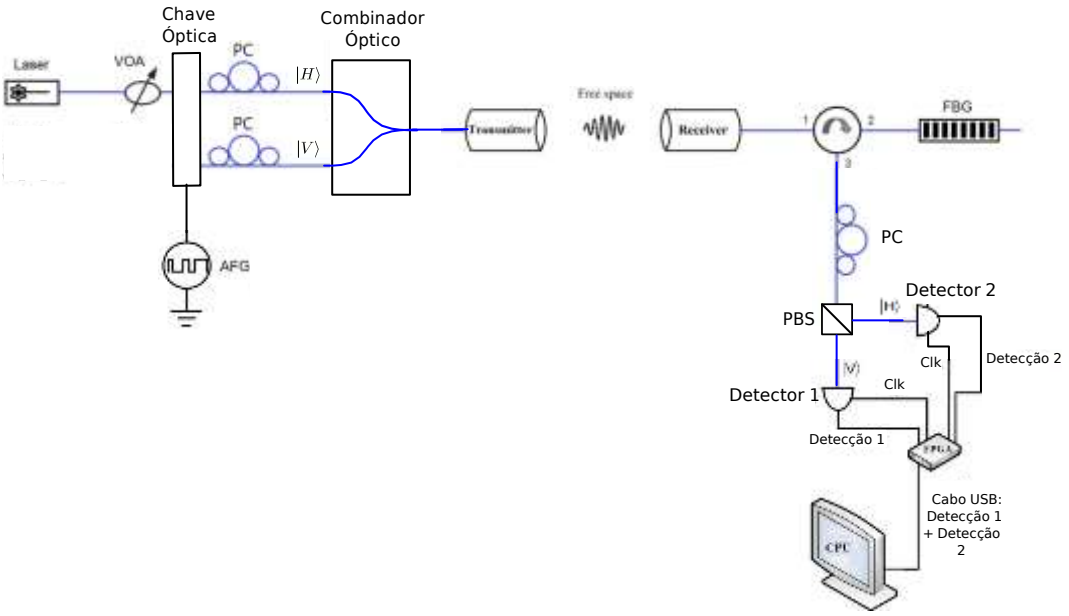


Figura 4.7: Terceiro setup experimental: codificação em polarização, utilizando chave óptica para seleção dos bits e ajuste extra no receptor.

Como a polarização da luz varia durante sua passagem pela fibra óptica, a luz que chega ao PBS do receptor pode estar em qualquer polarização, ainda que as polarizações originalmente ortogonais permaneçam ortogonais, uma vez que sofrem, em geral, as mesmas variações, por passarem pelo mesmo caminho óptico. Assim sendo, é necessário ajustar o PC do receptor a fim de alinhar as polarizações recebidas com os eixos do PBS. Desta forma, o setup apresenta dois ajustes de polarização locais e nenhum à distância, cumprindo seu objetivo.

Apesar de solucionar o que se propôs, esta alteração introduz uma indesejável manobra de desconexão e reconexão do canhão transmissor. Foi então realizada uma nova alteração no setup.

4.5
Quarto Setup: PBS no Transmissor

Este quarto setup experimental apresenta apenas a modificação da forma de ajuste da polarização no transmissor e seu esquema é apresentado na figura 4.8. No transmissor, foi colocado um PBS antes da chave óptica e esta é usada de forma inversa à anterior: seleciona dentre duas entradas qual será transmitida para a única saída, como um multiplexador. Desta forma, as polarizações $|H\rangle$ e $|V\rangle$ estão sempre presentes nas entradas da chave óptica,

que simplesmente seleciona qual delas será transmitida. Na entrada do PBS foi colocado um PC, pois a polarização do laser não é alinhada com os eixos do PBS de forma satisfatória. Para este setup funcionar bem, é necessário que a luz na entrada do PBS esteja polarizada em $|+45\rangle$ ou $|-45\rangle$, para que cada saída do PBS apresente a mesma potência. Mas, desta forma, metade da potência óptica é direcionada para cada saída do PBS a todo momento e apenas uma delas é selecionada para transmitir e, assim, foi inserida uma perda de 50% de potência no sistema.

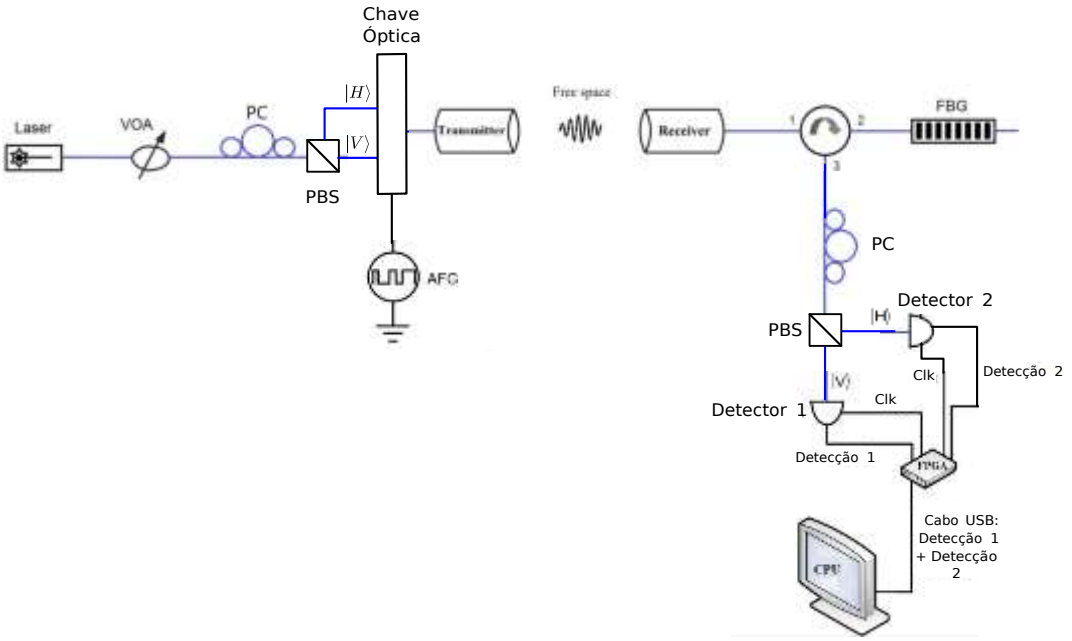


Figura 4.8: Quarto setup experimental: codificação em polarização, utilizando chave óptica para seleção dos bits e um PBS para ajuste das polarizações no transmissor.

Este setup alcançou a solução pretendida, porém, introduziu um problema que não existia antes. Há dois caminhos diferentes entre o PBS e a chave óptica percorridos pelos qubits $|H\rangle$ e $|V\rangle$, sem ajuste individual de polarização. Em cada um desses caminhos, existe uma variação diferente na polarização da luz e, desta forma, o que é efetivamente transmitido não são polarizações ortogonais.

4.6 Quinto Setup: O Definitivo

Transmissor

Até esse momento, o setup que melhor atendia a este trabalho era o terceiro setup, cujo problema introduzido (desconexão e reconexão do canhão

durante ajuste) é possível de conviver no sistema, ainda que não seja a situação ideal. Neste ponto no desenvolvimento do trabalho já seria possível realizar o experimento ao ar livre, realizando o enlace óptico entre os dois edifícios. Porém, ainda persiste a lentidão de resposta da chave óptica como empecilho ao desempenho óptico do sistema. Enquanto o receptor pode operar em frequências de 100 kHz *a* 1 MHz, a chave óptica limita o transmissor a algo em torno de 60 Hz.

A solução encontrada para aumentar a velocidade de chaveamento do transmissor foi a utilização de um controlador de polarização que não fosse mecânico. Dois tipos de controladores de polarização foram cogitados: um fabricado pela empresa EOSpace[11] e um pela Boston Applied Technologies (BATI[12]).

O EOSpace possui seis canais de ajuste de polarização, que não são necessariamente alinhados a eixos da esfera de Poincaré e, portanto, seu ajuste não segue uma lógica amigável. A única forma exequível em tempo aceitável de encontrar e obter repetibilidade de ajustes de estados de polarização ortogonais seria utilizando um polarímetro, como descrito em [60]. Conforme já mencionado na seção 4.3, este equipamento encontrava-se temporariamente indisponível no laboratório. Deste modo, os testes realizados com o controlador EOSpace foram considerados infrutíferos logo no início e o BATI foi selecionado para utilização neste trabalho, pois possui quatro estágios, sendo dois alinhados com o eixo S_1 da esfera de Poincaré e os outros dois alinhados com o eixo S_2.

O setup para o transmissor é apresentado na figura 4.9. O VOA tem a mesma função de ajustar a potência do laser para que o sistema opere em regime quântico. O PC e o BATI trabalham em conjunto, para que sejam ajustados os dois estados de polarização ortogonais. Primeiro, mantendo-se as três tensões no BATI em 0 V, ajusta-se o PC para obter a polarização $|V)$ na saída do PBS do receptor. Em seguida, sem alterar o ajuste do PC, encontram-se os valores de tensão nas fontes DC correspondentes para obter a polarização $|H)$ (outra saída do PBS do receptor) com o BATI . O procedimento de calibração do sistema é apresentado com mais detalhes na seção 5.2.

A seleção dos bits transmitidos, mais uma vez, é feita pelo AFG com as sequências de bits pseudo-aleatórias, mas, desta vez, o AFG não atua diretamente no elemento seletor/controlador de polarização. O BATI requer tensões relativamente altas, da ordem de 150 V, que o AFG não é capaz de gerar. Foi, então, projetado um circuito de controle, cuja entrada são as tensões

[11] Para detalhes sobre as características do controlador de polarização EOSpace, consulte a referência [59] e para detalhes sobre o funcionamento, a referência [60].

[12] Características do controlador de polarização BATI podem ser encontradas em [61] e [62].

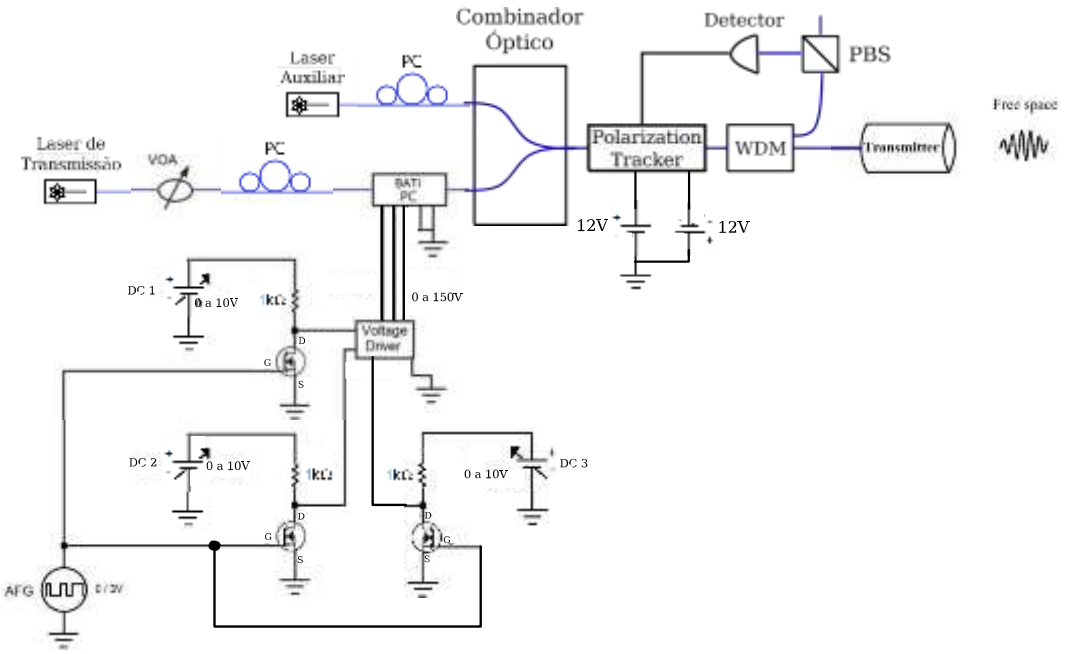


Figura 4.9: Quinto setup experimental: codificação em polarização com controle das polarizações por controlador automático – o setup definitivo do transmissor.

correspondentes aos bits clássicos 0 e 1 geradas pelo AFG, de 0 *V* e 3 *V*, respectivamente, e as saídas são as tensões de até 150 *V* para entrada no BATI. A saída do AFG está ligada aos pinos *gate* de três MOSFETs operando no modo *on-off*. Os pinos *source* dos MOSFET estão ligados à referência do sistema (ground), enquanto os pinos *drain* estão ligados através de resistores a três fontes ajustáveis de tensão DC. Quando tivermos nível alto na saída do AFG, a saída dos MOSFET será a referência (0 *V*), pois o MOSFET estará em modo *on* e, ao contrário, quando a saída do AFG for nível baixo, o MOSFET estará em *off* e a sua saída apresentará a mesma tensão que sua fonte de alimentação no *drain*, seja qual for esta tensão.

Conectado à saída dos três MOSFET, está um elevador de tensão (voltage driver) de 3 canais, um canal para cada MOSFET. O elevador de tensão é capaz de multiplicar por quinze as tensões de entrada em seus canais, de forma independente. Como as fontes de alimentação dos MOSFET podem ser ajustadas para valores de 0 a 10 *V*, temos saídas de 0 a 150 *V*. Estas são conectadas aos terminais de controle do BATI. Assim sendo, temos, efetivamente, o AFG selecionando as entradas do BATI entre 0 *V* ou a tensão ajustada até 150 *V* para cada canal.

Com a saída óptica do BATI ligada diretamente ao canhão transmissor, o sistema funcionou bem em bancada, em configuração back-to-back, pois o laboratório é um ambiente controlado, com temperatura constante, sem ventos e sem movimentação das fibras ópticas envolvidas no processo, logo, a

polarização da luz na fibra e nos equipamentos não varia tão significativamente no tempo, sendo necessários apenas reajustes no intervalo de alguns minutos.

Já para a instalação no telhado do edifício, foi necessário utilizar um cabo de fibras ópticas com 128 *metros* de comprimento, cujos últimos 46 *metros* foram dispostos no telhado, em área externa, sujeito a ventos e grandes variações de temperatura. Estas intempéries são capazes de fazer variar a polarização da luz dentro da fibra inúmeras vezes por segundo e de forma aleatória, o que tornaria impossível a calibração do sistema experimental como projetado. Foi, então, necessário, criar um mecanismo para superar esta dificuldade quando da transmissão entre edifícios. A solução foi a colocação de um regulador de polarização (Pol Tracker[13]) localizado fisicamente o mais próximo possível do canhão transmissor, no telhado.

O Pol Tracker atua através da maximização de um sinal elétrico (0*,* 5 a 4*,* 6 *V*), recebido de um detector óptico, cuja entrada recebe uma amostra da luz cuja polarização se quer controlar. Caso o laser de transmissão fosse utilizado para este feedback, o Pol Tracker tentaria seguir as duas polarizações em alternância pelos bits codificados, não sendo efetivo em manter nenhuma das duas. Para o funcionamento efetivo deste equipamento, foi utilizado um laser auxiliar, em outro comprimento de onda. Ainda dentro do laboratório, localizado fisicamente o mais próximo possível do BATI, foi colocado um combinador óptico para que o laser de transmissão e o laser auxiliar passassem a se propagar pela mesma fibra óptica. Desta forma, qualquer variação de polarização que o laser auxiliar sofrer na fibra óptica de 128 *m* até o Pol Tracker, o laser de transmissão também sofrerá, igualmente, a mesma variação. Assim, quando o Pol Tracker controlar seus motores para manter estável a polarização do laser auxiliar, estará igualmente mantendo estável a polarização do laser de transmissão. Ainda que o AFG esteja realizando o chaveamento entre duas polarizações ortogonais, cada uma delas será mantida, pois sua relação com a polarização do laser auxiliar não será alterada.

Na saída do Pol Tracker foi colocado um WDM, para separar os lasers pela diferença em seus comprimentos de onda e garantir que somente o laser de transmissão seja encaminhado ao canhão, enquanto somente o laser auxiliar retorna para feedback. Foi colocado um PBS no canal de feedback para que a polarização maximizada pelo Pol Tracker seja determinada.

O uso de fibra óptica mantenedora de polarização em lugar da fibra óptica *standard* seria suficiente para substituir todo o sistema associado ao Pol Tracker e ainda compensar a influência negativa causada pelo vento no sistema (contraste imperfeito de polarização – ver seção 5.5.2), porém, seu

[13]O manual do Pol Tracker pode ser obtido em [63].

altíssimo custo acaba por ser proibitivo para seu uso.

Receptor

Como pode ser observado na figura 4.10, para este setup não foram feitas alterações no sistema do receptor. Conforme mencionado anteriormente, a rede de Bragg filtra os ruídos provenientes do ambiente em comprimentos de onda diferentes dos de interesse, necessitando estar acoplada a um circulador, pois ela reflete o comprimento de onda de interesse.

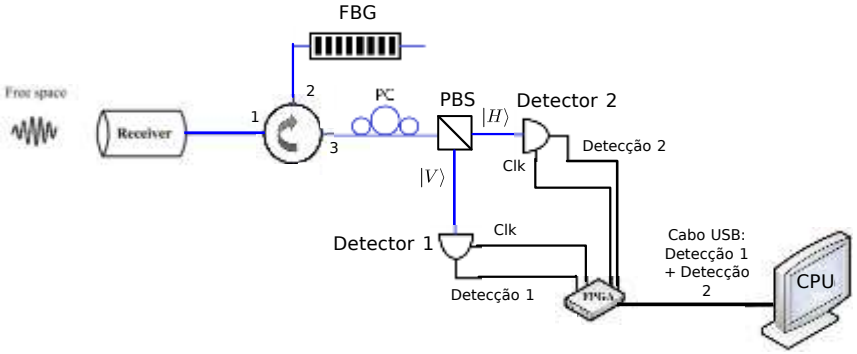


Figura 4.10: Quinto setup experimental: codificação em polarização com controle das polarizações por controlador automático – o setup definitivo do receptor.

O PC é utilizado para alinhar a polarização dos fótons recebidos com os eixos do PBS, que separa os fótons recebidos de acordo com a sua polarização, enviando cada polarização para um detector diferente, e os SPAD detectam efetivamente os fótons recebidos, sendo um para os fótons em $|H\rangle$ (SPAD-0) e outro para os fótons $|V\rangle$ (SPAD-1). A FPGA gera o *clock* para os SPAD e coleta e armazena em memória volátil cada pulso gerado por eles ao detectarem um fóton. O Computador programa a FPGA em cada inicialização e coleta, armazena e interpreta os dados inicialmente armazenados na memória da FPGA. A fase de interpretação dos dados não é feita *online*, isto é, não ocorre durante a transmissão, mas sim como um processo separado, posteriormente.

Este setup foi montado em bancada, realizando o enlace back-to-back, e testado exaustivamente. Os procedimentos de calibração e de transmissão e os dados coletados são apresentados no capítulo 5. Após os testes em bancada, o sistema foi montado entre edifícios e foram realizadas transmissões ao ar livre, sob a influência dos agentes externos. Os resultados também são apresentados e discutidos no capítulo 5.

5
Experimentos e Resultados

Nestes experimentos, o protocolo BB84 não foi realizado em sua completude, uma vez que não foi colocado um dispositivo para troca de bases e, portanto, não foram utilizadas duas bases não-ortogonais entre si. Foi utilizada apenas a base $|V\rangle, |H\rangle$ tanto no transmissor quanto no receptor. Do ponto de vista da segurança da informação, o uso de apenas uma base seria desastroso, caso este fosse um sistema QKD comercial. Eva poderia obter o mesmo conhecimento que Bob sobre a chave. Mas, como o objetivo deste trabalho é provar princípios e realizar um estudo do canal, isto não será um problema. No protocolo original, como proposto por Bennett e Brassard, as escolhas das bases, tanto por Alice, quanto por Bob, são feitas aleatoriamente, logo, estatisticamente, cada base será usada 50% das vezes por cada um deles. Assim, metade das medidas de ambos serão na mesma base e a outra metade (que será descartada) em bases diferentes. Desta forma, as taxas de bits conseguidas neste trabalho são, estatisticamente, o dobro das que seriam conseguidas utilizando o BB84 original completo, pois uma perda adicional da ordem de 50% seria esperada referente às vezes em que Alice e Bob escolhem (aleatoriamente) bases diferentes para suas medidas. Em realidade, o uso das duas diferentes bases em 50% das vezes cada uma, como proposto por Bennet e Brassard, já caiu por terra ainda na década de 1990. A quantidade relativa de vezes em que as bases são usadas pode ser qualquer uma que se deseje, desde que se mantenha a escolha aleatória entre elas, ainda que com probabilidades diferentes de serem escolhidas. Assim, a perda adicional de 50% mencionada acima é apenas o pior caso. Isso em nada diminui a validade dos resultados aqui obtidos, uma vez que as polarizações que efetivamente se propagam tanto na fibra óptica quanto na atmosfera são várias, já que a polarização dos fótons varia dentro da fibra. O simples fato de termos que calibrar o sistema receptor, através do ajuste do PC, a cada poucos minutos nos mostra que diferentes bases de polarizações ortogonais estão efetivamente sendo transmitidas via espaço livre e/ou na fibra óptica do receptor, após acoplamento no canhão. Logo, a configuração experimental resultou mais simples do que se tivéssemos que incluir um sistema para mudanças de base com a rapidez e precisão requeridas, sem que tivéssemos perda de generalidade na prova de princípios pretendida e no

estudo dos fenômenos ocorridos no espaço livre.

É importante notar ainda que, para este trabalho, foi admitido que o estabelecimento das chaves é realizado através do canal quântico, via o formato apresentado para QKD, com conciliação da chave via canal clássico, e que a transmissão da informação criptografada com a chave estabelecida se dá por um canal clássico qualquer sem ruído, ou seja, o canal não induz erros adicionais na mensagem que não aqueles já introduzidos pelas diferenças nas chaves de Alice e Bob. Não há perda de generalidade nesta suposição, uma vez que os arquivos criptografados podem, por exemplo, ser gravados em um *pen drive* ou em um DVD e entregues ao destinatário. Estes canais não introduzem erros na mensagem. Ademais, a consideração de inserção de erros durante a transmissão da mensagem já criptografada em nada acrescentaria à realização dos objetivos deste trabalho.

Neste capítulo é discutida a utilização do setup definitivo para realização do enlace híbrido de comunicação óptica para transmissão de dados em regime quântico, passando por todas as etapas de ajustes do sistema até a apresentação e discussão dos resultados obtidos. Na seção 5.1 é descrito como os canhões foram alinhados entre si, tanto para o arranjo *back-to-back* quanto a 160 m de distância, em edifícios diferentes. A seção 5.2 apresenta o procedimento de calibração do sistema para a transmissão dos dados, explicando de que forma são alinhadas as polarizações ortogonais da luz, $|H)$ e $|V)$. O procedimento para utilização do código em MATLAB a fim de identificar os dados recebidos e compará-los com os dados transmitidos é apresentado na seção 5.3. E nas seções 5.4 e 5.5 são relatados e discutidos os resultados obtidos, respectivamente, nas configurações *back-to-back* no laboratório e ao ar livre entre edifícios.

Para todos os experimentos com o setup definitivo, foram utilizadas nos SPAD a eficiência máxima de 25%, o clock na frequência de 1 MHz e a duração da janela de detecção de 5 ns. Isto significa que, a cada 1 μs, o SPAD polariza o fotodetector próximo ao estado de avalanche durante 5 ns. Janelas mais largas que estas geram um aumento maior de contagens de escuro do que de detecções, piorando, assim, a relação sinal-ruído.

Para o transmissor, há uma limitação de resposta no tempo do BATI, cuja especificação técnica garante que cada estágio consegue estabilidade da polarização em um tempo da ordem de 30 μs para cada variação de π rad. Portanto, a frequência máxima de operação é de 33,33 kHz. De forma conservadora, foi escolhida a frequência máxima de 25 kHz para o clock do transmissor. A cada um bit transmitido, o receptor estaria detectando 40 bits iguais.

A diferença entre as velocidades de clock nas duas pontas do enlace é, para dizer o mínimo, um problema para a segurança da informação em um link cujo objetivo seja estabelecer uma chave secreta para uso em criptografia. Se cada 40 bits detectados são iguais, Eva poderia, a partir da interceptação de poucos bits, identificar um padrão na sequência transmitida sem inserir perturbações detectáveis no canal e reconstruir a informação com qualidade suficiente para ter uma chave tão semelhante à de Alice e Bob que a possibilitaria decifrar qualquer mensagem trocada entre eles. Mas, como o objetivo deste trabalho envolve a prova de princípios e não necessariamente o efetivo estabelecimento de chaves secretas para utilização, os experimentos aqui realizados não ficam prejudicados por estas repetições de bits no receptor. Pode-se utilizar o entendimento que a sequência da Alice, ao invés de possuir 200 bits, possui 8000 bits, sendo eles iguais 40 a 40 e que o clock do tranmissor é igual ao do receptor. Com este entendimento, o sistema e a transmissão com a finalidade de estabelecer a chave secreta podem ser avaliados, partindo-se do princípio que a sequência aleatória de bits utilizada é que é ruim, por estar longe de ser realmente aleatória, mas a resposta do sistema a uma chave aleatória (ou pelo menos pseudo-aleatória) seria a mesma que a obtida pela sequência ruim e a chave seria estabelecida de forma satisfatória.

Uma forma de possibilitar o aumento da velocidade de resposta do sistema pode ser a inserção de vários BATI em série. Desta forma, cada um deles seria responsável pela variação parcial da polarização de entrada, obtendo-se na saída do conjunto a polarização ortogonal à da entrada. Por exemplo, fazendo-se uma aproximação para entendimento do raciocínio, se forem utilizados três BATI em série, cada um deles será responsável pela rotação de um terço da rotação necessária para a obtenção da polarização ortogonal e, portanto, seu tempo de resposta seria reduzido para um terço do tempo para a variação completa, o que possibilitaria triplicar o clock do transmissor. A inclusão de mais BATI e testes com essa configuração ficam como sugestão para trabalhos futuros, uma vez que, durante o período de desenvolvimento deste trabalho, só havia um dispositivo destes disponível no laboratório. Outra possibilidade seria a utilização do controlador de polarização EOSpace, calibrado com o uso de um polarímetro. Este equipamento possui tempo de resposta menor que o BATI, da ordem de 100 *ns*, o que possibilitaria um clock de até 10 *MHz* no transmissor.

Ainda que a diferença entre clocks seja prejudicial para a segurança da informação, ela traz uma vantagem experimental. Para simplificar a implementação física do sistema devido ao exíguo tempo para desenvolvimento experimental, os clocks do transmissor e do receptor não são sincronizados e não

há um protocolo para início e fim da transmissão, como, por exemplo, uma sequência de bits de *start*, assim, quando o receptor começa a registrar as medições, o bit que está sendo transmitido no momento pode ser qualquer um dentre os 200 bits da sequência que se repete. Caso houvesse uma correspodência de equivalência, de cada bit transmitido representar um bit no receptor, a identificação de qual é o bit inicial detectado dentre os 200 bits da sequência pseudo-aleatória seria uma tarefa árdua, tendo em vista que no mínimo 75 % dos bits são perdidos devido à máxima eficiência dos SPAD, o que gera no receptor, após o descarte das janelas vazias, uma sequência de bits que é um subconjunto desconhecido da sequência transmitida. O fato de cada bit transmitido representar 40 bits iguais na sequência registrada no receptor facilita sobremaneira essa identificação.

Pode-se evitar esta necessidade de identificação de algumas formas. Uma solução seria a transmissão, no mesmo sistema, de um laser de sincronismo, em outro comprimento de onda, com potência compatível com transmissão clássica, utilizando os mesmos canhões transceptores, com a inclusão de um WDM no receptor para separar o sinal de sincronismo do sinal de dados. Desta forma, os SPAD iniciariam a detecção exatamente ao mesmo tempo em que é transmitido o primeiro bit da sequência e os clocks se manteriam exatamente sincronizados durante toda a transmissão. Por se tratar de uma implementação física em paralelo com este trabalho e pela necessidade de desenvolvimento de mais um código para a FPGA tratar o sinal óptico de clock e transformá-lo efetivamente em sinal elétrico de clock para os SPAD, esta fica como mais uma sugestão para trabalhos futuros.

5.1
Procedimento de Alinhamento dos Canhões Transceptores

O alinhamento feito em bancada, para a configuração *back-to-back*, é muito simples e pode ser realizado por um indivíduo sozinho. Como a distância entre os canhões transceptores é de apenas 1,60 *m*, é possível fazer um alinhamento grosso a olho nu, sem precisar de laser algum. Após isto feito, injeta-se o laser infravermelho no canhão transmissor e faz-se o ajuste fino dos canhões medindo-se a potência na saída da fibra óptica do receptor. O alinhamento termina quando se maximiza a potência lida no instrumento.

Já para o alinhamento dos canhões transceptores nos telhados dos edifícios, foram necessárias duas pessoas: uma localizada junto ao transmissor e outra junto ao receptor. Alguns artifícios foram utilizados a fim de facilitar o trabalho e obter a melhor performance dos sistemas, uma vez que a distância entre as extremidades do enlace torna difícil a vista precisa de detalhes de um

ponto ao outro, como pode ser visto na figura 5.1.

Figura 5.1: Local de instalação do canhão transmissor, com visada para o local de instalação do receptor (indicado pela seta amarela). Na foto, o canhão receptor encontra-se instalado no local e é possível notar a dificuldade de visualização a olho nu.

Cada canhão transceptor teve de ser alinhado com informações da pessoa de instalação da outra ponta do enlace via telefone celular e foi efetuado com um laser em um comprimento de onda visível (verde – 523 *nm*) à noite, pois durante o dia não é possível enxergar de forma satisfatória a luz do laser, devido ao ofuscamento causado pela luz do sol, que é de grande intensidade.

Primeiro, o laser visível foi projetado do transmissor sobre o receptor para alinhamento grosso de fixação dos suportes da estrutura e a parede atrás do canhão funcionou como anteparo para a luz verde. A pessoa posicionada no local utilizou a própria sombra do canhão receptor como fonte de informação para o alinhamento, como mostrado na figura 5.3. É possível notar, pela intensidade da luz, onde está localizado o centro do feixe projetado, o que facilita muito o alinhamento. O mesmo procedimento foi adotado para alinhamento grosso do canhão receptor, projetando-se o laser verde no sentido contrário, do receptor para o transmissor.

Depois de feito o alinhamento grosso, ainda com o laser verde, foi efetuado o alinhamento fino, controlando o nível de potência recebida, utilizando um medidor de potência óptica na fibra óptica de saída do canhão receptor, buscando maximizar a leitura no aparelho, enquanto eram feitos ajustes nos parafusos milimétricos dos canhões. É importante notar o quão fino deve ser este ajuste: cada $0,1^\circ$ de variação na angulação do transmissor causa aproximadamente 28 *cm* de variação do local atingido pela luz a 160 *m* de distância, o que é muito maior que o alvo (lente) a ser atingido pelo feixe, que

Figura 5.2: Visada para o local de instalação do transmissor a partir do receptor durante procedimento de alinhamento dos canhões com laser verde.

Figura 5.3: Processo de alinhamento dos canhões. À esquerda, canhões desalinhados. À direita, alinhamento grosso concluído.

tem $7,56\ cm$ de diâmetro. Após a conclusão do alinhamento, foi feita uma medição semelhante com o laser infravermelho e foi obtida uma potência da ordem de $-45\ dBm$, o que é considerada até alta para regime quântico. Desta forma, o alinhamento foi considerado concluído e ainda é necessário manter o VOA no transmissor para reduzir a potência até o regime quântico.

5.2
Procedimento de Calibração do Sistema e Transmissão

A figura 4.9 é aqui repetida como figura 5.4 para facilitar a leitura.

O primeiro ajuste de calibração das polarizações é feito por uma pessoa no transmissor, recebendo feedback de uma pessoa situada no receptor, observando as leituras nos dois SPAD. Mais uma vez, a comunicação entre eles é feita via telefone celular. Primeiramente, ajusta-se o PC do laser auxiliar para maximização do sinal de feedback do Pol Tracker próximo, mas abaixo, de $4,6\,V$, a fim de ele ser capaz de manter regulação mais precisa da polarização.

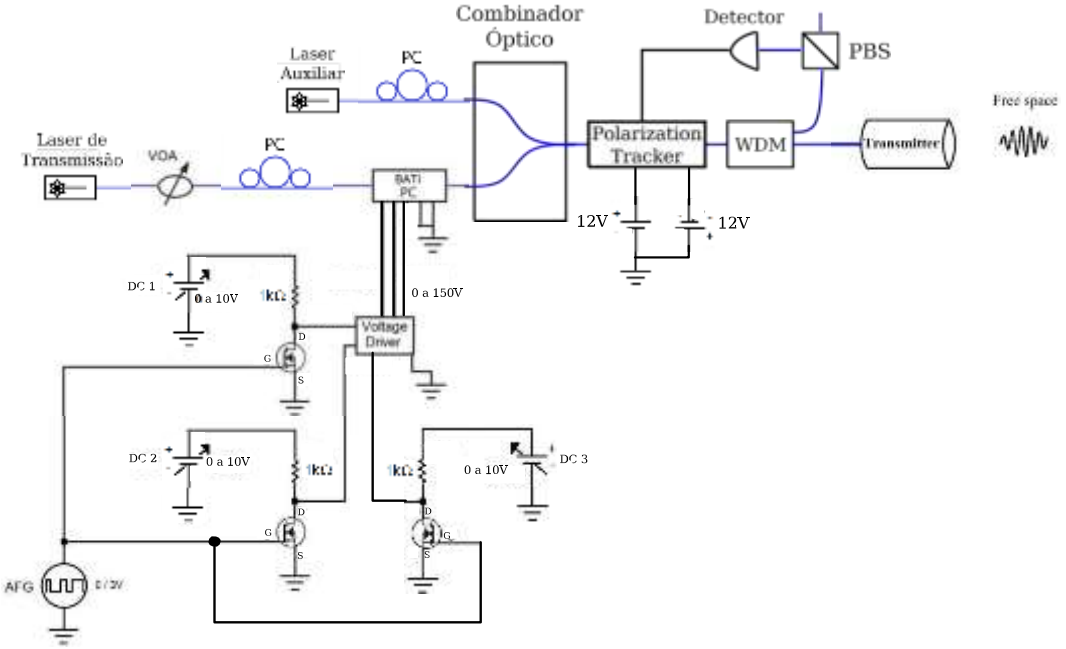


Figura 5.4: Setup experimental defintivo do transmissor.

Em seguida, com as três fontes de tensão DC ajustadas para $0\,V$, ajusta-se o PC do laser de transmissão para obter leitura mínima no SPAD-0 e leitura máxima no SPAD-1. Este será o qubit $|V\rangle$. Na sequência, mantendo-se o PC em posição, varia-se a tensão da fonte DC-1 até se obter um mínimo de leitura no SPAD-1. Este é um mínimo local. Varia-se então a tensão da fonte DC-2, também até ser obtido o mínimo local no SPAD-1. Por último, é variada a tensão da fonte DC-3 para obtenção do mínimo global no SPAD-1. Pode-se ainda repetir toda a operação de ajuste das tensões quantas vezes forem necessárias para fazer um ajuste fino da polarização, obtendo-se mínimo de leitura no SPAD-1 e máximo no SPAD-0. Isto significa que o BATI está girando a polarização de sua entrada em 90° e este será o qubit $|H\rangle$.

Após estes ajustes, as polarizações ortogonais já estão prontas para serem transmitidas. Quando no gerador de função for selecionado nível alto, os MOSFET estarão conduzindo e, portanto, em suas saídas teremos a referência

do sistema (0, 0 *V*) e, portanto, o *voltage driver* colocará os mesmos 0, 0 *V* na entrada do BATI, ou seja, a polarização ajustada no PC do laser de transmissão está passando pelo BATI sem sofrer alteração, representando os qubits $|V)$. Inversamente, quando no AFG for selecionada a saída de nível baixo, os MOSFET estarão em modo de corte e em suas saídas estarão as tensões das fontes DC associadas a cada um deles. Desta forma, o *voltage driver* colocará, em cada entrada do BATI, as tensões ajustadas anteriormente para a polarização ortogonal, ou seja, o BATI está gerando rotação de 90° na polarização de sua entrada, representando os qubits $|H)$.

A transmissão propriamente dita se dá ao selecionar, no AFG, nível alto entre 2, 5 e 3, 5 *V*, nível baixo entre 0, 0 e 1, 0 *V* e forma de onda arbitrária com a sequência de bits pseudo-aleatória desejada. A recepção se inicia (ou se interrompe) quando selecionada no computador a opção *start measurement* (ou *stop measurement*). A cada vez que a memória da FPGA fica cheia, as informações são automaticamente descarregadas para o computador e salvas em dois arquivos de texto, um contendo as sequências de detecções do SPAD-0, sendo as detecções representadas por "1" e as ausências de detecções representadas por "0", e o outro contendo as sequências de detecções do SPAD-1. Como cada janela aberta pelos detectores recebe um bit de representação, inclusive aquelas em que não há detecção, a comparação entre os resultados dos SPAD é direta. Mais detalhes sobre esta interpretação dos dados são apresentados na Seção 5.3. Por motivos explicados juntamente com a interpretação dos dados obtidos, as transmissões foram realizadas em "rajadas" de vinte segundos cada.

Como já mencionado anteriormente, as polarizações ajustadas nos PC e no BATI não são necessariamente horizontal e vertical, mas sim duas polarizações ortogonais quaisquer que, após passarem por todo o sistema e sofrerem todas as variações por este imposta, mantêm-se ortogonais e chegam ao PBS do receptor alinhadas com sues eixos, sendo, então, enviadas para cada um dos SPAD de acordo com a sua polarização inicial. Estas são então interpretadas, por simplificação de raciocínio, como $|H)$ e $|V)$.

5.3
Procedimento de Análise dos Dados

Ao fim das transmissões, temos dois arquivos para cada "rajada" de vinte segundos, um tendo os conteúdos de cada janela de detecção aberta pelo SPAD-0 e outro contendo a mesma coisa para o SPAD-1, sendo as detecções representadas por "1" e as ausências de detecções representadas por "0". Ou seja, cada arquivo tem uma sequência de "0" e "1" relacionada às detecções de

cada SPAD. Por exemplo, se o milionésimo bit do arquivo relativo ao SPAD-0 for um "0" e o milionésimo bit do arquivo do SPAD-1 for um "1", isto significa que, no instante $t = 1\,s$, o SPAD-0 não sinalizou detecção, enquanto ao mesmo tempo o SPAD-1 sinalizou uma detecção, uma vez que o clock utilizado nos SPAD foi de $1\,MHz$.

Para cada instante de detecção, podemos ter quatro resultados diferentes, conforme mostrado na Tabela 5.1. Se um dos SPAD indica uma detecção numa determinada posição e o outro não indica na mesma posição, será interpretado como um qubit detectado por aquele SPAD. As posições em que os SPAD apresentam a mesma indicação, seja ausência de detecção ao mesmo tempo ou presença de detecção ao mesmo tempo, são consideradas janelas de detecção perdidas e não são associadas a nenhum qubit. Como o objetivo da transmissão é o estabelecimento de uma chave aleatória secreta de comprimento arbitrário, composta de uma sequência de bits, podemos descartar as janelas perdidas no receptor e os bits correspondentes a elas na sequência transmitida, bastando, para isso, realizar uma conciliação, uma vez que, como já mencionado anteriormente, uma subsequência aleatória de bits é ainda uma sequência aleatória de bits, ainda que mais curta.

Tabela 5.1: Interpretação dada às possíveis combinações de detecção dos SPAD.

SPAD-0	SPAD-1	INTERPRETAÇÃO DO QUBIT DETECTADO
0	0	janela vazia, sem detecção
0	1	$\|V)$
1	0	$\|H)$
1	1	influência da contagem de escuro

A primeira ação computacional, implementada em MATLAB, para interpretação dos dados coletados é identificar qual era a posição do primeiro bit registrado na sequência recebida dentro da sequência pseudo-aleatória transmitida, como já mencionado na primeira parte deste capítulo. A segunda ação é o descarte, pelo transmissor, de todos os bits referentes às janelas de detecção perdidas, mediante conciliação com o receptor. E, por último, para avaliar a qualidade da transmissão realizada, é feita a comparação entre a sequência de bits resultante no transmissor e a sequência de bits resultante no receptor. Após esta comparação, alguns parâmetros são calculados.

São eles:

(a) QBER da transmissão[1];

[1] A QBER é calculada como a quantidade de bits da chave de Bob que divergem da chave

(b) Taxa de bits por segundo obtidos para a chave;
(c) Quantidade de bits na chave estabelecida;
(d) Porcentagem de janelas de detecção que foram aproveitadas para o estabelecimento da chave;
(e) Porcentagem de janelas perdidas por ausência de detecção; e
(f) Porcentagem de janelas perdidas por indicação simultânea de detecção.

5.4
Resultados Experimentais Back-to-Back

Foram realizadas inúmeras transmissões (mais de 800, no total) com o setup definitivo em configuração *back-to-back* em ambiente controlado, no laboratório, com o objetivo de caracterizar o sistema antes da instalação dos canhões transceptores nos telhados. As diferenças medidas posteriormente, ao ar livre, são, então, atribuídas aos elementos externos, como luz do sol, vento, chuva e névoa. Esta seção primeiro apresenta o experimento e seus resultados e, na sequência, uma simulação do uso das chaves para criptografia e descriptografia de textos e imagens.

5.4.1
Estabelecimento e Análise das Chaves Obtidas em Back-to-Back

Inicialmente, foram medidas as perdas em cada componente do transmissor, cuja perda total associada medida foi de 69,0 *dB* (somando-se a atenuação dos componentes – 10,1 *dB* – e a atenuação ajustada no VOA – 58,9 *dB*), para esta montagem, sem o combinador óptico, o Pol Tracker e o WDM. Na atenuação associada aos componentes, já estão incluídas as perdas associadas às lentes, da ordem de 0,9 *dB*, medidas em laboratório.

A figura 5.5 mostra a curva característica para a transmissão da lente de Borosilicato (BK7), utilizada como lente objetiva nos canhões transceptores. Percebe-se que a perda teórica associada às lentes objetivas é de 0,457 *dB* para o comprimento de onda de 1,55 *µm*. Já as lentes oculares apresentam transmitância de 99,75% para o mesmo comprimento de onda[2], o que corresponde a uma atenuação de 0,011 *dB*. Ou seja, a atenuação teórica associada às lentes é de 0,468 *dB*. A atenuação medida experimentalmente foi maior devido ao desgaste do revestimento da lente objetiva devido ao longo período em que ela ficou exposta ao tempo.

de Alice, dividida pela quantidade total de bits das chaves.

[2] O datasheet das lentes pode ser obtido em https://www.thorlabs.com/thorproduct.cfm?partnumber=F230FC-1550.

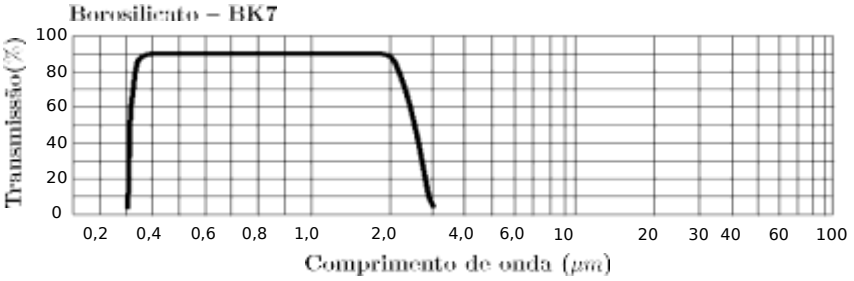


Figura 5.5: Curva teórica para a característica de transmissão da lente de Borosilicato utilizada nos canhões transceptores [26].

Em seguida, foram caracterizadas as perdas no receptor (exceto o SPAD), cujo valor total obtido foi de 17,0 *dB*. O maior contribuinte para esta perda, considerada alta, é a conexão da fibra óptica multimodo do canhão receptor com a fibra monomodo do circulador (6,5 *dB*), pois, como o diâmetro do núcleo da fibra multimodo é muito maior e sua abertura numérica também, parte da energia é lançada fora do núcleo da fibra monomodo. Esta é uma perda com a qual temos que conviver, uma vez que a troca da fibra óptica multimodo por uma monomodo no canhão induziria uma perda muito maior no sistema devido à ineficiência de acoplamento da luz oriunda do espaço livre na fibra óptica. Já a troca das fibras ópticas monomodo do sistema por fibras multimodo é inviável, pois os componentes ópticos utilizados foram os componentes comerciais típicos, disponíveis no laboratório, todos eles já acoplados de fábrica a fibras ópticas monomodo. Nos 17,0 *dB* citados, também já estão incluídas as perdas por reflexão nas lentes do canhão e por não acoplamento à fibra óptica, medidas em bancada da ordem de 1,5 *dB*. Novamente, a perda é maior que a teórica devido ao desgaste da lente objetiva.

Nos SPAD, há dois fatores contribuintes para perdas. Em primeiro lugar, a eficiência quântica do detector é de 25%, ou seja, insere uma perda de 6 *dB*. Em segundo lugar, com o clock de *M Hz*, temos uma janela aberta a cada 1 *μs*, mas a janela fica aberta somente durante 5 *ns*, o que dá um *duty cycle* de 1/200, isto é, uma perda de 23 *dB*, totalizando 29 *dB* de perda no SPAD. Foi realizado um experimento para a confirmação da atenuação causada pelo SPAD. Utilizando um laser com potência conhecida e dois atenuadores ópticos variáveis em série, foi variada a atenuação de um dos VOA, sempre de forma a obter baixíssimas potências (conhecidas) na entrada do SPAD e, a partir da taxa de detecção apresentada pelo SPAD, foi calculada a atenuação. Na média, foi obtida uma atenuação bastante próxima dos 29 *dB* teóricos, inclusive para leitura de 27 *kHz*, a mesma que obtivemos nas transmissões durante o dia.

Foram realizadas medições com um medidor de potência óptica de espaço

livre (OPM) situado junto à lente do canhão transmissor e depois situado a 1, 60 *m* de distância, na posição do receptor. Em ambas as situações, o OPM apresentou aproximadamente a mesma leitura de potência, logo, as perdas associadas à propagação no espaço livre em um espaço tão curto e em local abrigado podem ser consideradas desprezíveis.

O experimento consistiu na transmissão de diversas sequências pseudo-aleatórias de bits em várias combinações diferentes de potência no transmissor e de tempo de duração da transmissão. Foram feitas transmissões de duração de 3; 5; 10; 20; 30; 40; 50 e 60 segundos e potências correspondentes a 0,10; 0,17; 0,25; 0,33; 0,40 e 0,50 fótons por janela temporal de detecção. Após a conciliação de janelas válidas, a porcentagem de bits errados (diferentes de uma sequência para a outra) nos fornece a QBER. A figura 5.6 apresenta o gráfico da QBER em função do tempo de transmissão para as diversas potências utilizadas. Cada valor do gráfico representa a média de todos os valores obtidos para cada par potência–tempo de transmissão.

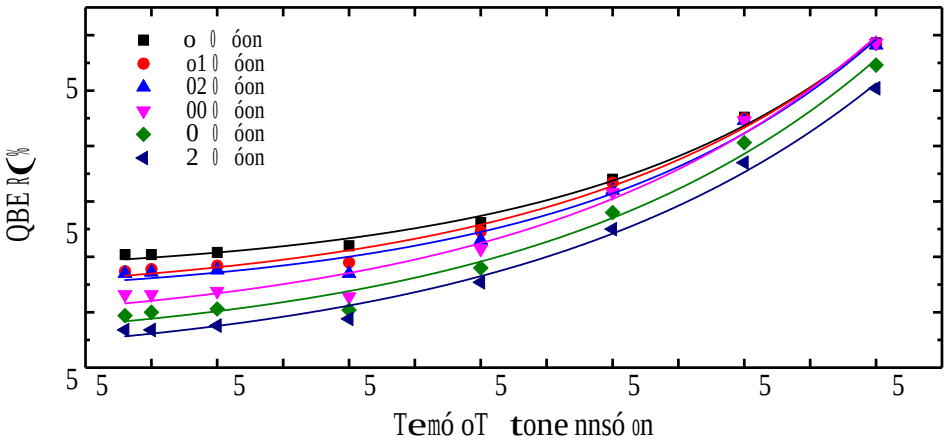


Figura 5.6: QBER em função do tempo de duração de uma transmissão para seis potências de transmissão diferentes.

Percebe-se que, independente da potência utilizada, o comportamento da curva é o mesmo: crescimento exponencial da QBER com o aumento do tempo de transmissão. Este comportamento é explicado pela falta de sincronismo entre as duas pontas do enlace. Os clocks do transmissor e do receptor não são exatamente iguais e não iniciam exatamente no mesmo instante. Assim, por mais que a diferença entre clocks resida apenas a partir da quinta casa decimal, após determinado tempo começa a haver interferência intersimbólica, gerando interpretação errônea de bit no receptor e, consequentemente, aumentando a taxa de erro.

A partir destes resultados, depreende-se que o melhor tempo de transmissão para esta configuração é de 20 segundos, pois não há ganho significativo

na taxa de erro das transmissões mais curtas, enquanto há um aumento considerável na QBER para conexões mais longas.

Utilizando-se, então, os dados obtidos para transmissões de duração de 20 segundos, foi comparada a sequência de bits recebida com a sequência de bits transmitida, após conciliação de janelas válidas. O resultado obtido para as diferentes potências utilizadas é exibido na figura 5.7. Como mencionado no capítulo 3, em regime quântico, historicamente utiliza-se, em média, 0, 1 fóton por pulso a ser transmitido, não sendo, entretanto, essencial este valor, pois caso utilizados os *decoy states*, podes-se usar médias bem maiores. Foram, então, testadas também outras potências, para avaliar a influência da quantidade de fótons na taxa de erro. Ao conhecimento do autor, a comunidade científica tem conseguido obter QBER da ordem de 3%[3] e pode-se observar no gráfico que, em geral, as taxas obtidas neste trabalho são compatíveis com este valor, variando, de 2, 94% a 3, 60%, a depender da potência utilizada. Cabe ressaltar que, neste trabalho, a potência utilizada foi a equivalente a 0, 1 fótons por pulso medidos na entrada do SPAD, por janela temporal de detecção aberta, considerando que a utilização da técnica de *decoy states*, caso implementada, seria suficiente para a defesa contra ataques PNS eventualmente realizados por Eva.

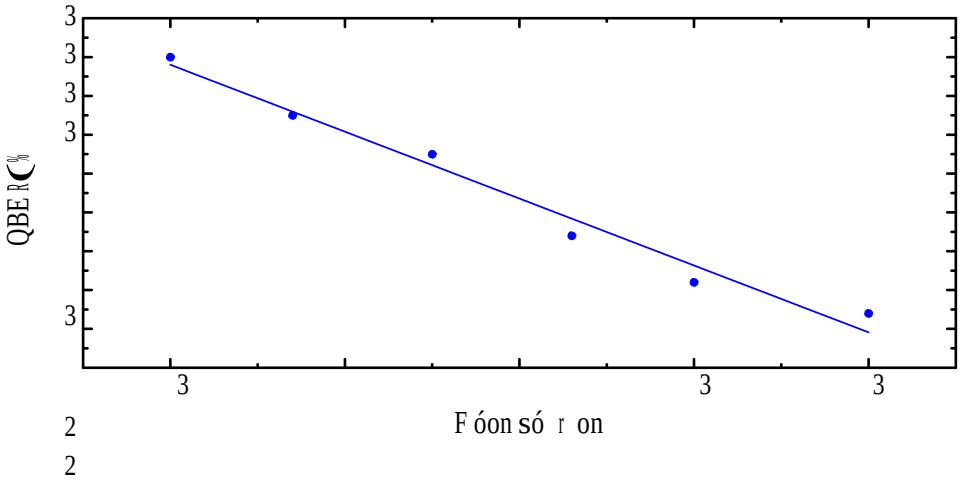


Figura 5.7: QBER em função da potência transmitida, para transmissões de 20 segundos de duração.

As taxas de transmissão médias obtidas, em kbits por segundo, para cada potência utilizada são mostradas na figura 5.8. Estes dados representam a taxa de bits válidos recebidos, após a conciliação feita com o transmissor, mas ainda antes da execução de qualquer algoritmo de amplificação de privacidade. Há descarte de bits sempre que é feita amplificação de privacidade, diminuindo

[3]Alguns exemplos podem ser encontrados em [18], [64], [65], [66] e vários outros artigos publicados.

a chave sensivelmente e, portanto, as taxas efetivas são significativamente menores.

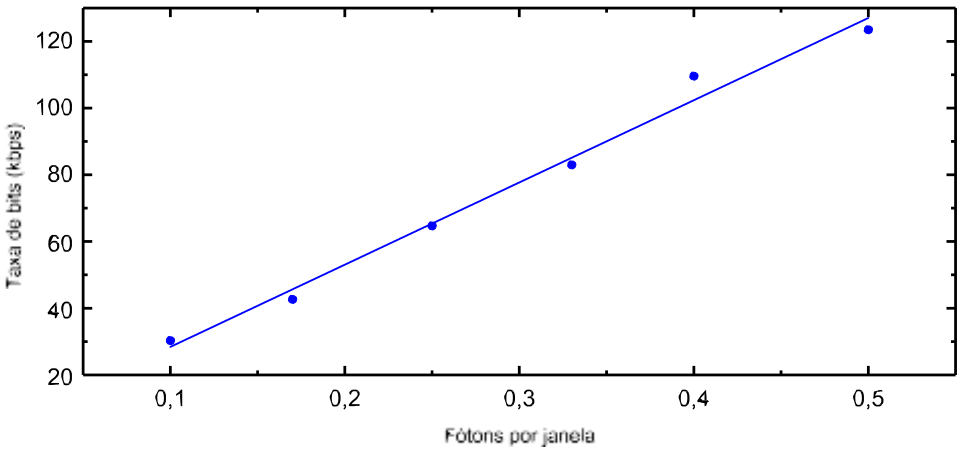


Figura 5.8: Taxa de bits obtida para a chave criptográfica em função da potência de transmissão.

Para uma potência equivalente a 0,1 fóton por janela de detecção, a taxa média obtida foi de 30,33 *kbps*, o que gera, em média, 606,6 *kbits* de chave criptográfica a cada rajada de vinte segundos. Ou seja, para criptografar uma imagem colorida (RGB) padrão de 1024 × 768 *pixels*, sem considerar amplificação de privacidade, seriam necessárias 31 "rajadas" de 20 segundos de sequências pseudo-aleatórias de bits, correspondendo a um total de 10 minutos e 20 segundos de transmissão de qubits para se obter uma chave do mesmo tamanho da mensagem. Já para criptografia de mensagens de texto, uma transmissão de 20 segundos é capaz de gerar chave para criptografar mensagens com até 75825 caracteres.

Ainda a partir dos dados experimentais, a taxa média obtida de janelas perdidas por ausência de detecção foi de 969,67 mil janelas por segundo ou 96,967% das janelas, enquanto a taxa de janelas perdidas por indicação simultânea de detecção foi menor que 0,004% em todos os casos.

5.4.2
Utilização das Chaves Obtidas em Back-to-Back para Criptografia

Este método não se mostrou eficaz para a transmissão de mensagens de texto, pois cada caracter é representado por 8 bits (código ASCII) e basta um erro em um desses bits para alterar completamente a mensagem. Por exemplo, o código ASCII da letra **"t"** é 01110100 (116). Se o terceiro bit menos significativo for errado devido à chave criptográfica, o **"t"** será descriptografado como um "p" (01110000 – 112), ou se for alterado o segundo bit mais significativo ele será descriptografado como um "4" (00110100 – 52). Desta forma, uma criptografia em bits que representam códigos ASCII

apresentam uma capacidade de "amplificar" a taxa de erro em até 8 vezes, caso todos os erros ocorram em bits de caracteres diferentes. Obviamente, se erros se agruparem dentro de um mesmo caracter, esse *fator multiplicador* diminui.

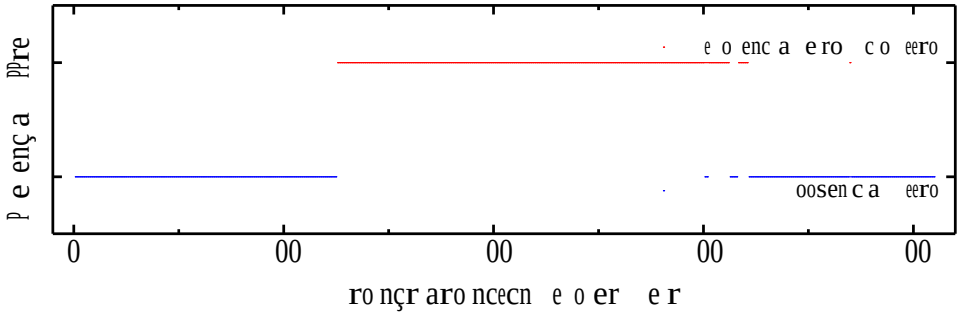


Figura 5.9: Localização dos caracteres errados (em vermelho) em uma mensagem contendo 410 caracteres no total.

A figura 5.9 mostra a distribuição de erros para uma mensagem de texto criptografada utilizando uma das chaves obtidas experimentalmente: em vermelho a localização, dentro da mensagem, dos caracteres que contêm pelo menos um bit errado. Neste exemplo, nota-se que 46, 59% dos caracteres apresentam erro. Esta é uma mensagem curta, com apenas 410 caracteres, logo, para este caso, só foram utilizados os primeiros $410 \times 8 = 3280$ bits dos 606, 6 *kbits* totais da chave (apenas 0, 54% da chave). A QBER para esta chave completa foi de 3, 19%, mas, para o trecho dela utilizado na criptografia desta mensagem, foi de 5, 83%, pois havia mais erros no trecho inicial da chave. O *fator multiplicador* para este caso foi de 7, 99, quase máximo. O resultado da comunicação pode ser visto na figura 5.10. Não é difícil perceber que a mensagem descriptografada, à direita na figura, está ininteligível.

Figura 5.10: À esquerda, mensagem original a ser criptografada. À direita, mensagem descriptografada com chave recebida.

No segundo exemplo, visto na figura 5.11, foi utilizada uma mensagem de 1000 caracteres a ser criptografada. Neste caso, foi utilizada a mesma chave que no caso anterior, mas apenas 19, 40% dos caracteres apresentaram erros.

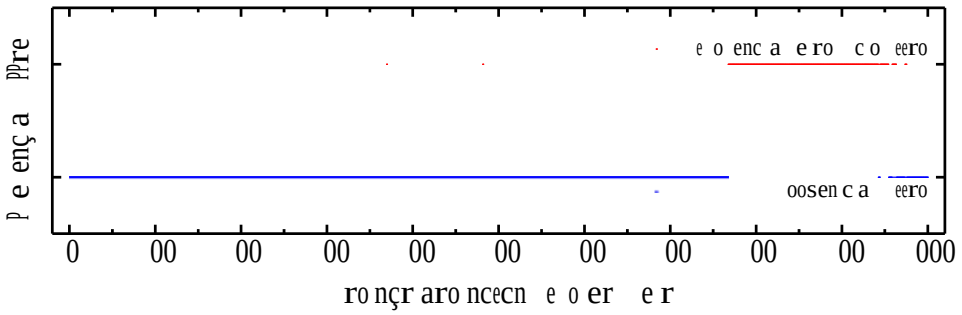


Figura 5.11: Localização dos caracteres errados (em vermelho) em uma mensagem contendo 1000 caracteres no total.

Para este exemplo, foram utilizados os primeiros $1000 \times 8 = 8000$ bits dos 606, 6 *kbits* totais da chave (1, 32% da chave, bem mais que no caso anterior). Como dito acima, a QBER para esta chave completa foi de 3, 19%, mas, para o trecho dela utilizado na criptografia desta segunda mensagem foi de 3, 95%, o que nos dá um *fator multiplicador* de 4, 91, pois os erros ficaram mais agrupados dentro de caracteres, ou seja, proporcionalmente, mais caracteres apresentaram mais de um bit errado do que no caso anterior.

Mais uma vez o resultado da comunicação é demonstrado (ver figura 5.12). O resultado obtido é muito melhor que no caso anterior, visto que é possível entender do que se trata, ler a placa do carro e o código renavam e outras informações. Entretanto, o resultado ainda é ruim. Os números do código de barras para pagamento estão ininteligíveis, logo, é impossível pagar este boleto. Na verdade, bastaria que um dígito do código tivesse sido corrompido para que isto acontecesse.

Uma solução é a transmissão de imagens criptografadas ao invés de textos criptografados.

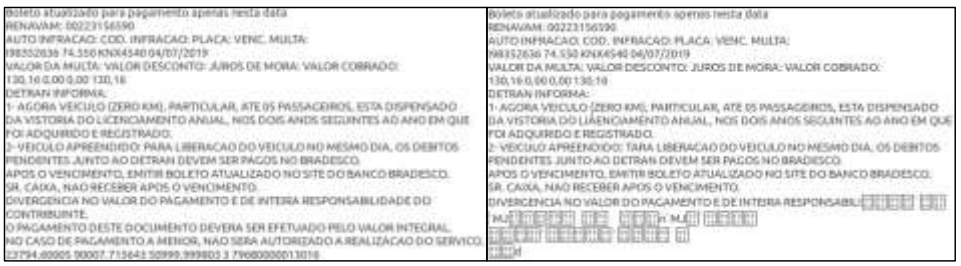


Figura 5.12: À esquerda, mensagem original a ser criptografada. À direita, mensagem descriptografada com chave recebida.

As imagens coloridas padrão são compostas de três matrizes (um tensor) em que cada uma delas representa uma das três cores básicas, vermelho, verde e azul (RGB – red, green, blue). Cada posição de cada matriz representa a intensidade da cor a que a matriz corresponde, codificada em 256 níveis de

intensidade. Ou seja, em cada posição do tensor existe um número entre 0 e 255. Esta quantidade de números pode ser codificada em 8 bits. Assim, uma imagem de 1024×768 pixels, um dos tamanhos padrão para monitores de computador, será representada por um tensor de dimensões $1024 \times 768 \times 3$, que, por sua vez, possuirá $1024 \times 768 \times 3 \times 8 = 18.874.368$ bits, o que corresponde aproximadamente a 31 chaves de 20 segundos de transmissão. Desta forma, a QBER obtida será a média das QBER das 31 chaves utilizadas, independentemente do fato dos erros estarem ou não concentrados em determinadas regiões.

Ambas as mensagens utilizadas nos exemplos anteriores foram transformadas em imagens e foi aplicado o mesmo procedimento de criptografia/descriptografia aplicado anteriormente. Os resultados são apresentados nas figuras 5.13 e 5.14. No primeiro caso, a taxa de erro foi de 3,58%, enquanto no segundo foi de 3,76%.

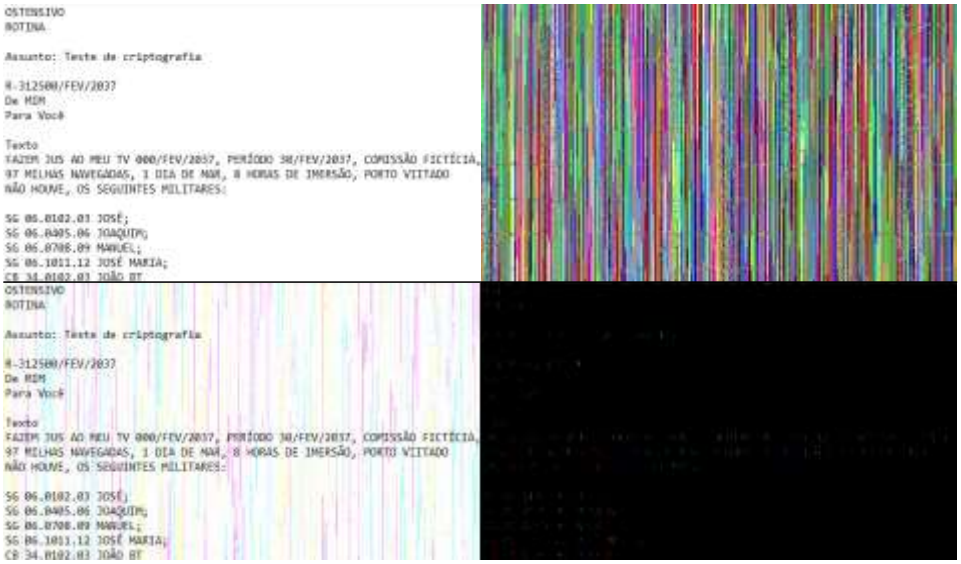


Figura 5.13: À esquerda acima, mensagem original a ser criptografada. À direita acima, mensagem criptografada. À esquerda abaixo, mensagem descriptografada com chave recebida. À direita abaixo, erros (diferenças entre as mensagens original e descriptografada).

É fácil perceber a melhoria no resultado da qualidade na transmissão da mensagem[4]. Não há dificuldade no entendimento de qualquer um dos caracteres que seja, nas duas mensagens. É perfeitamente possível ao destinatário, no caso do boleto (figura 5.14), digitar os números do código de barras em um caixa eletrônico ou aplicativo do banco e pagar a conta. Mas, como transformamos

[4]Entenda-se por qualidade na transmissão da mensagem o fato de que o destinatário entende corretamente e completamente o conteúdo da mensagem.

o texto em imagem, poderíamos enviar o próprio código de barras junto com seu código numérico. Será que funciona?

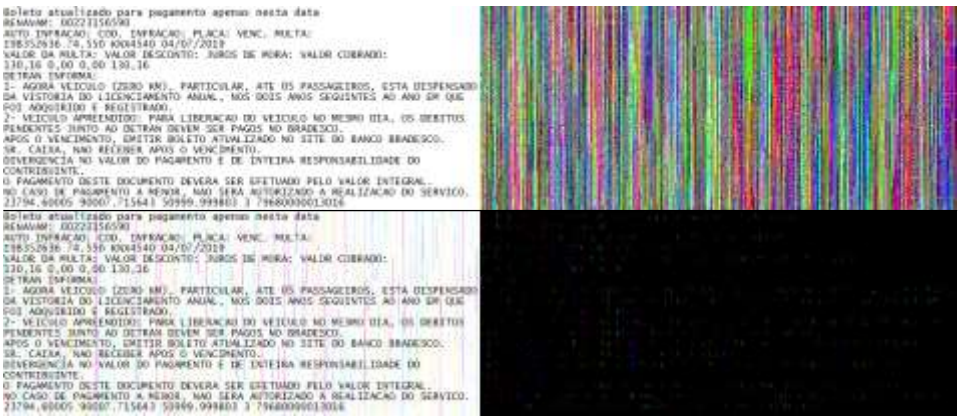


Figura 5.14: À esquerda acima, mensagem original a ser criptografada. À direita acima, mensagem criptografada. À esquerda abaixo, mensagem descriptografada com chave recebida. À direita abaixo, erros (diferenças entre as mensagens original e descriptografada).

Foi, então, realizada uma criptografia da imagem do boleto incluindo o código de barras (figura 5.15). Nota-se que o resultado foi semelhante ao obtido nos dois casos anteriores. E, de forma surpreendente, o leitor do código de barras do aplicativo do celular foi capaz de ler o código da mensagem descriptografada!

Do ponto de vista da efetividade da comunicação entre Alice e Bob, enquanto as transmissões de caracteres de texto falharam, as transmissões de imagens foram um sucesso. Mas ainda precisamos analisar esta comunicação quanto à segurança da informação.

Se considerarmos, conservadoramente, que todo o ruído do sistema foi introduzido por Eva, a máxima informação que Eva pode obter sobre a mensagem, em cada caso, é dada pela imagem inferior à direita nas figuras 5.13, 5.14 e 5.15, que apresenta as diferenças entre as imagens originais e suas correspondentes criptografadas/descriptografadas. A potência utilizada neste trabalho foi maior que aquela equivalente a $\mu = 0,1$ fótons por pulso se propagando no espaço livre, mas, com o uso da técnica de decoy states, Alice e Bob podem monitorar o canal e conseguem detectar a presença de Eva e evitar o ataque PNS, descartando a chave, se for o caso.

Nos dois primeiros casos, percebemos que Eva não possui meios de extrair qualquer informação a partir dos pontos em que ela obteve conhecimento. Não há qualquer figura formada naquelas imagens. Já no terceiro caso, pode-se ver um esboço de código de barras. Mas o nosso conhecimento prévio de que há um código de barras ali torna a avaliação tendenciosa. Provavelmente, quem não

Figura 5.15: À esquerda acima, mensagem original a ser criptografada. À direita acima, mensagem criptografada. À esquerda abaixo, mensagem descriptografada com chave recebida. À direita abaixo, erros (diferenças entre as mensagens original e descriptografada).

sabe *a priori* sobre a presença do código de barras na imagem, não associaria aquele esboço ao que ele realmente é. Ainda assim, saber que existe um código de barras na imagem dá a Eva o conhecimento sobre o tipo de mensagem trocada, mas não sobre o conteúdo. Assumindo que não queremos que Eva tenha informação nem ao tipo de mensagem, basta, mais uma vez, executar um dos algoritmos de amplificação de privacidade para que Eva tenha tão pouca informação quanto se queira, uma vez que a QBER foi abaixo de 12% (na verdade, da ordem de três vezes menor).

Levantou-se ainda a hipótese da transmissão de fotos ser capaz de revelar mais informação à Eva do que a imagem de textos. A partir dessa hipótese, foram feitos os procedimentos de criptografia/descriptografia para várias imagens diferentes, utilizando-se chaves de diferentes QBER, mas sempre em torno da média obtida de 3,60%.

Passemos então a um exercício: a figura 5.16 apresenta a informação disponível para Eva no caso da transmissão de seis imagens diferentes. Observe as seis imagens e responda às seguintes perguntas: É possível identificar o conteúdo das mensagens? É possível identificar pelo menos o assunto ou o tipo de mensagem? As QBER obtidas no estabelecimento das chaves utilizadas para o procedimento foram: (a) 3,28%; (b) 3,62%; (c) 3,59%; (d) 3,61%; (e) 3,70% e (f) 3,46%. Nota-se que em algumas das imagens é possível ter uma ideia do que se trata, mas isso tem mais a ver com as características da própria imagem

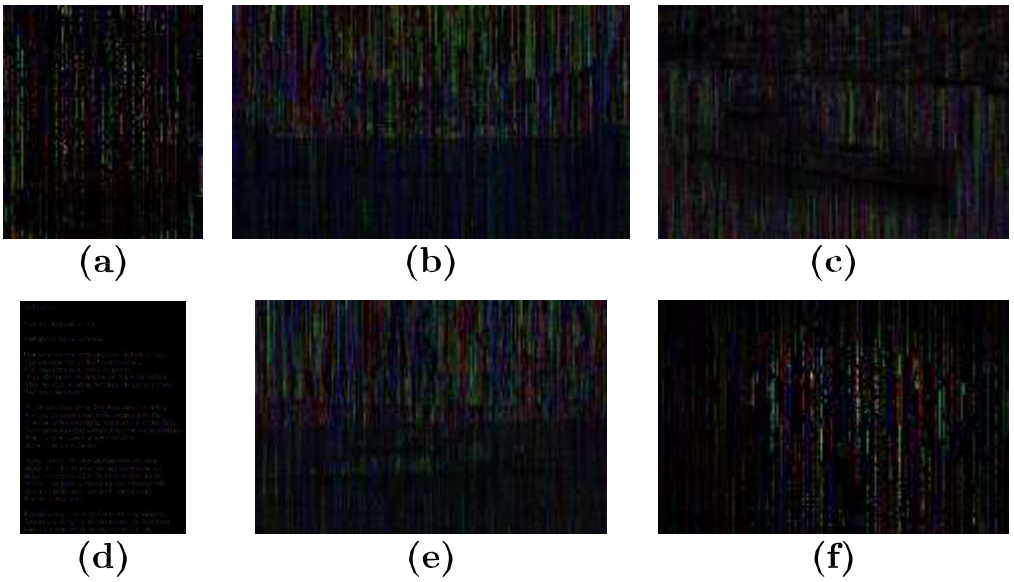


Figura 5.16: Conhecimento máximo de Eva sobre as mensagens de seis transmissões criptografadas realizadas a partir de chaves estabelecidas neste experimento.

do que com a QBER das chaves utilizadas.

Para facilitar um pouco o exercício, vamos dar alguma ideia sobre o conteúdo de cada uma das imagens. Elas são de: uma fragata, uma corveta, um navio de transporte de tropas e veículos, uma lâmpada em fundo escuro, uma imagem de Buda e um poema. Qual das imagens de Eva pertence a cada uma destas mensagens?

As respostas são mostradas nas figuras (a) 5.17 – Buda; (b) 5.18 – fragata; (c) 5.19 – navio de transporte; (d) 5.20 – poema; (e) 5.21 – corveta; (f) 5.22 – lâmpada.

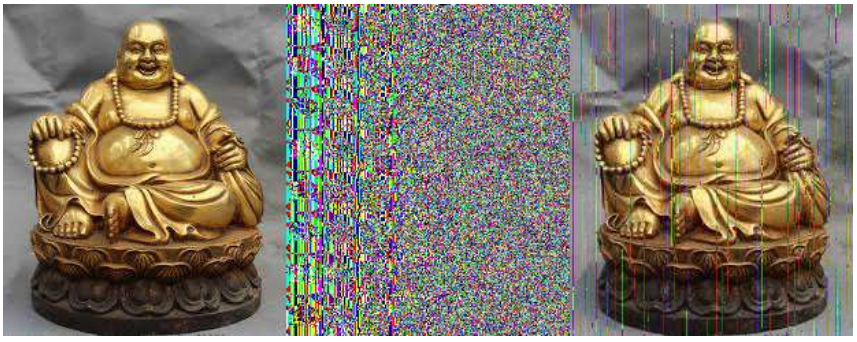


Figura 5.17: Imagens original, criptografada e descriptografada de uma estatueta de Buda.

Em todas as tríades de imagens das figuras 5.17 até 5.22, nota-se que a imagem criptografada realmente não contém informação útil alguma para quem não conhece a chave capaz de descriptografá-la.

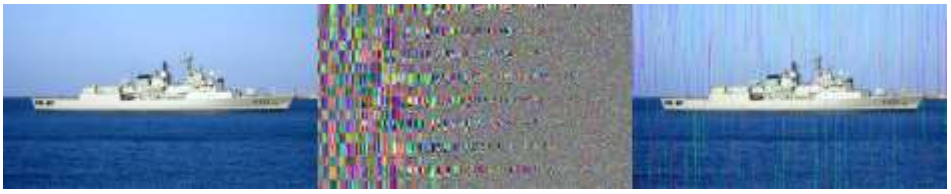
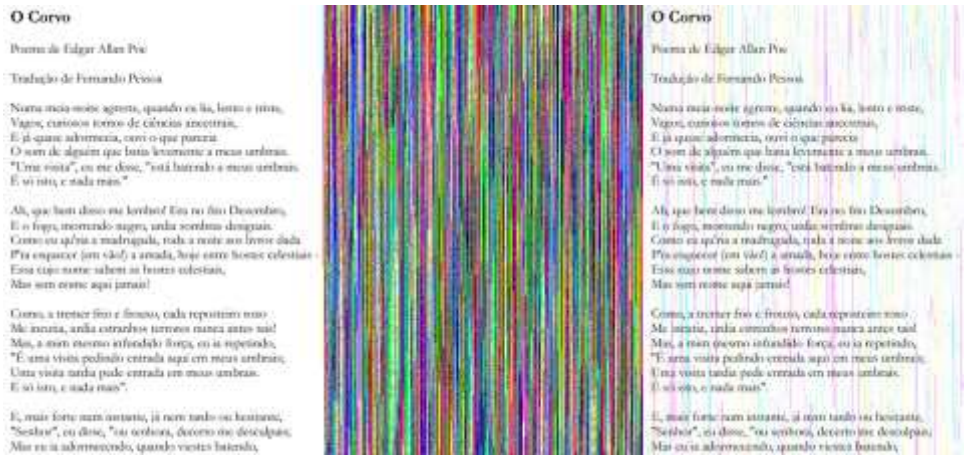


Figura 5.18: Imagens original, criptografada e descriptografada de uma fragata.

Figura 5.19: Imagens original, criptografada e descriptografada de um navio de transporte de tropas e veículos.



O Corvo

Poema de Edgar Allan Poe

Tradução de Fernando Pessoa

Numa meia-noite agreste, quando eu ia, lento e triste,
Vagos, curiosos tomos de ciências ancestrais,
E já quase adormecia, ouvi o que parecia
O som de alguém que batia levemente a meus umbrais.
"Uma visita", eu me disse, "está batendo a meus umbrais.
É só isto, e nada mais."

Ah, que bem disso me lembro! Era no frio Dezembro,
E o fogo, morrendo negro, unha sombras desiguais.
Como eu qu'ria a madrugada, toda a noite aos livros dada
P'ra esquecer (em vão!) a amada, hoje entre hostes celestiais
Essa cuja norte sabem as hostes celestiais,
Mas sem nome aqui jamais!

Como, a tremer frio e frouxo, cada reposteiro roxo
Me incutia, unha estranhos terrores nunca antes sais!
Mas, a mim mesmo infundido força, eu já repetindo,
"É uma visita pedindo entrada aqui em meus umbrais;
Uma visita tarda pede entrada em meus umbrais.
É só isto, e nada mais".

E, mais forte num instante, já nem tardo ou hesitante,
"Senhor", eu disse, "ou senhora, decerto me desculpais;
Mas eu ia adormecendo, quando vestes batendo,

O Corvo

Poema de Edgar Allan Poe

Tradução de Fernando Pessoa

Numa meia-noite agreste, quando eu ia, lento e triste,
Vagos, curiosos tomos de ciências ancestrais,
E já quase adormecia, ouvi o que parecia
O som de alguém que batia levemente a meus umbrais.
"Uma visita", eu me disse, "está batendo a meus umbrais.
É só isto, e nada mais."

Ah, que bem disso me lembro! Era no frio Dezembro,
E o fogo, morrendo negro, unha sombras desiguais.
Como eu qu'ria a madrugada, toda a noite aos livros dada
P'ra esquecer (em vão!) a amada, hoje entre hostes celestiais
Essa cuja norte sabem as hostes celestiais,
Mas sem nome aqui jamais!

Como, a tremer frio e frouxo, cada reposteiro roxo
Me incutia, unha estranhos terrores nunca antes sais!
Mas, a mim mesmo infundido força, eu já repetindo,
"É uma visita pedindo entrada aqui em meus umbrais;
Uma visita tarda pede entrada em meus umbrais.
É só isto, e nada mais".

E, mais forte num instante, já nem tardo ou hesitante,
"Senhor", eu disse, "ou senhora, decerto me desculpais;
Mas eu ia adormecendo, quando vestes batendo,

Figura 5.20: Imagens original, criptografada e descriptografada de um poema.

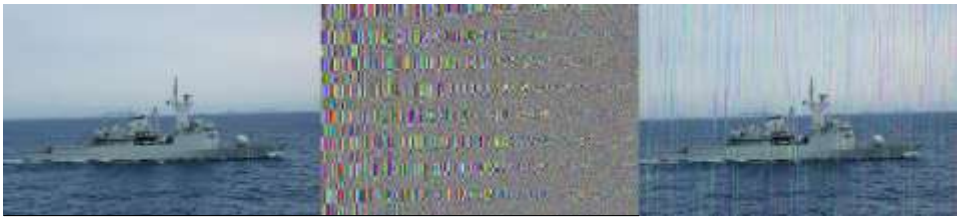


Figura 5.21: Imagens original, criptografada e descriptografada de uma corveta.

Podemos, ainda, proceder a mais uma comparação. Para textos convertidos em imagem, onde as cores não são importantes, podemos convertê-los em imagem em preto e branco e obtemos o seguinte resultado: imagens coloridas vazam mais informação que imagens em tons de cinza (ainda que o efeito não seja tão acentuado) como pode ser visto nas figuras 5.23 a 5.25.

Figura 5.22: Imagens original, criptografada e descriptografada de uma lâmpada em fundo escuro.

Figura 5.23: Comparação entre a informação obtida por Eva para imagem colorida *versus* imagem em preto e branco para o boleto com código de barras.

Figura 5.24: Comparação entre a informação obtida por Eva para imagem colorida *versus* imagem em preto e branco para a mensagem informativa.

Isto decorre do fato que, em uma imagem colorida, possuímos 3 informções para cada pixel da imagem: vermelho, verde e azul. Mesmo que Eva só consiga obter informação sobre uma destas componentes, apesar dela não conseguir formar a cor correta para aquele pixel, ela tem *alguma* informação sobre ele. Assim, estamos na realidade criptografando três versões da imagem e Eva pode obter mais informação que os simples 3,60% fornecidos pela QBER ao superpor as três imagens. No limite, caso cada subimagem fornecesse a Eva informação sobre pixels diferentes, sem superposição, ela poderia obter até 10,80% de informação sobre a imagem. Na prática, sempre há superposição de pixels e Eva nunca chega aos 10,80% teóricos. Em uma imagem em preto em branco (ou tons de cinza, para ser mais preciso), só há uma informação sobre cada pixel. Se Eva não obtiver esta informação, não obtém informação

Figura 5.25: Comparação entre a informação obtida por Eva para imagem colorida *versus* imagem em preto e branco para o poema.

alguma. Portanto, o máximo de informação obtida será mesmo 3, 60%. Um efeito colateral benéfico da transformação da imagem de colorida em tons de cinza é que a chave necessária para a criptografia passa a ser três vezes menor.

Mais uma vez, observando as figuras, percebemos que Bob é capaz de compreender completamente a mensagem que Alice queria transmitir, enquanto Eva tem informação marginal sobre o conteúdo da mensagem, mostrando, novamente, a aplicabilidade prática do esquema de distribuição de chaves quânticas com codificação de qubits em polarização da luz infravermelha para a criptografia de imagens. Com o uso dos algoritmos de amplificação de privacidade, a informação marginal que Eva possui sobre o conteúdo da mensagem (ou das imagens) passa a ser quase inexistente. Ela pode ser feita arbitrariamente pequena, ao custo da diminuição da taxa de transmissão de bits.

Estando a configuração do sistema validada, todos os patâmetros entendidos após os experimentos em ambiente controlado e todos os procedimentos testados e aprimorados, partimos, então, para os experimentos ao ar livre, instalando o enlace para comunicação entre dois edifícios, a 160 *m* de distância.

5.5

Resultados Experimentais ao Ar Livre

Após a validação do sistema em configuração back-to-back, os canhões foram instalados a 160 *m* de distância, nos telhados de dois edifícios do campus da PUC-Rio para o estudo do sistema de QKD verdadeiramente em espaço livre, sujeito às oscilações e variações impostas pelas intempéries que a atmosfera impõe. Em primeiro lugar, esta seção apresenta os testes com o filtro da luminosidade solar e a caracterização de sua influência no sistema. Em seguida, são mostrados e discutidos os resultados experimentais das transmissões de qubits para estabelecimento de chaves criptográficas.

5.5.1
Caracterização da Distribuição da Luz Solar e Teste de Eficácia do Filtro

O primeiro passo para a realização do enlace ao ar livre foi a caracterização da distribuição da luz solar ao longo do dia no local de instalação e a medição da eficiência do filtro (a rede de Bragg). Para isso, o canhão receptor foi instalado no local destinado ao canhão transmissor (por questão de logística), no telhado do CETUC, dentro do campus da PUC-Rio (equivalente ao oitavo andar), e todo o sistema receptor foi acoplado a ele para realizações de medidas ao longo das 24 horas de vários dias, com condições climáticas diferentes. No total, foram 11 dias de medições nesta configuração, sendo cinco dias ensolarados sem a rede de Bragg no sistema, dois dias nublados sem a rede de Bragg no sistema, dois dias ensolarados com a rede de Bragg no sistema, dois dias nublados com a rede de Bragg no sistema. As configurações mencionadas são mostradas na figura 5.26.

A figura 5.27 mostra os resultados médios obtidos. Cada ponto no gráfico representa a média de cinco minutos de medições, indicando o número de contagens dado pelo SPAD por segundo. Os quadrados em vermelho indicam a média obtida para dias ensolarados sem filtragem da luz do sol. Percebe-se que o pico de luz captada pelo canhão e acoplada na fibra óptica acontece por volta das 10 horas e 30 minutos da manhã, momento em que o sol já está alto no céu e, portanto, está fora do campo de visão do sistema. Este fenômeno ocorre devido à reflexão em algum elemento do ambiente que está no campo de visão do canhão transceptor e, neste momento do dia, a triangulação geométrica sol – objeto – canhão faz com que a luz solar refletida no objeto incida diretamente na lente e com um ângulo menor que a abertura numérica da fibra óptica. Note, também, que este objeto é provavelmente côncavo e concentra a luz incidente, uma vez que a intensidade detectada é maior inclusive que a própria incidência direta da luz do sol, que ocorre mais tarde, por volta das 15 horas. Após este horário, o sol começa a ficar encoberto pelo morro presente no local e, mesmo

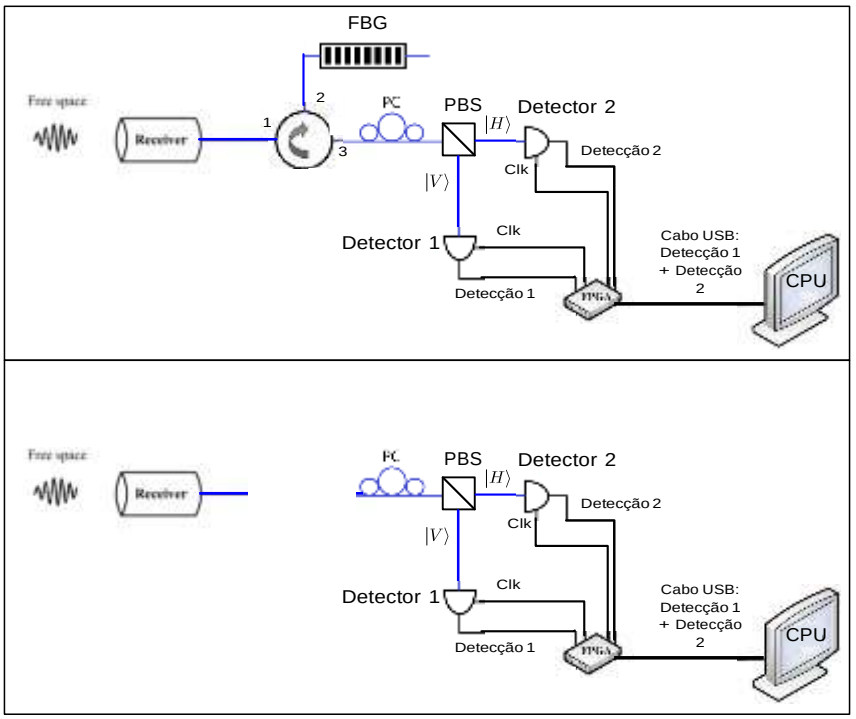


Figura 5.26: Esquemas do sistema receptor com o filtro para a luz solar (acima) e sem o filtro (abaixo).

que sua angulação seja mais favorável à detecção pelo sistema, sua intensidade total no local diminui. Ao fim da tarde há uma descontinuidade na envoltória do gráfico que se deve ao momento em que o sol se põe atrás do morro a oeste do campus, mas ainda resta um pouco de luz no ambiente, capaz de impressionar os detectores, até o momento em que o céu fica realmente escuro.

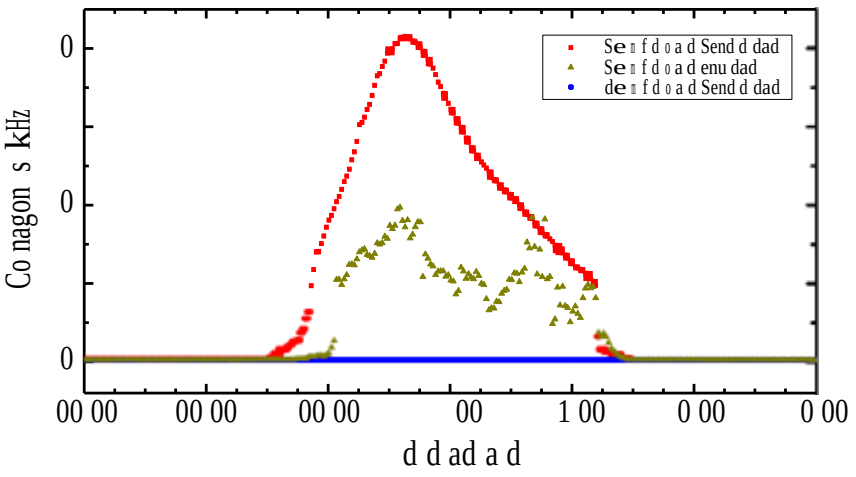


Figura 5.27: Comparação das medições da contagem de fótons para a luz do sol ao longo de 24 horas. Em vermelho, dia ensolarado sem filtro óptico, em dourado, dia nublado sem filtro óptico e em azul, dia ensolarado com filtro óptico.

A série de triângulos dourados no gráfico indica as médias das medições

em dias nublados, ainda sem o filtro. É fácil perceber que, do início da manhã até em torno do meio-dia, a envoltória segue o mesmo curso do dia ensolarado, mas com intensidade menor. Após o meio-dia, a distribuição de nuvens começa a variar, devido às diferenças entre os dias em que as médias foram realizadas e também devido aos ventos incidentes no local, empurrando nuvens diferentes para posições diferentes. Mesmo com essas variaçãoes, é possível perceber um máximo local perto de 15 horas, resultado do maior alinhamento do sol com o canhão transceptor. Existem duas descontinuidades na envoltória do gráfico dos dias nublados, uma no início da manhã e outra no final da tarde, cujas causas são distintas. A descontinuidade do início da manhã foi causada por nuvens escuras bloqueando a luz solar, em um dos dois dias de medições, e, posteriormente, sendo deslocadas pelo vento, dando lugar a nuvens menos carregadas. A do fim da tarde se deve ao mesmo motivo da descontinuidade em dias ensolarados: o morro localizado a oeste bloqueando o sol próximo ao horário do por do sol.

Ressalta-se que estas medidas foram realizadas em dias no entorno do equinócio (23 de setembro), quando os dias e as noites têm a mesma duração, pois o sol está localizado próximo à linha do equador. Como o campus da PUC-Rio está localizado na latitude 22,980 sul, a máxima elevação do sol no céu durante o equinócio representa uma inclinação de $90 - 22,980 \approx 67^\circ$ com relação ao zênite.

A série de círculos azuis no gráfico da figura 5.27, que visualmente parece uma linha azul, representa as médias das medições realizadas com o filtro, a rede de Bragg, em dias ensolarados. A eficácia da filtragem fica evidente, uma vez que a linha acompanha o zero da escala. Para uma visualização mais detalhada destes pontos, a figura 5.28 mostra somente eles, em uma escala mais apropriada, retirando do gráfico as medições realizadas sem o filtro.

Como era de se esperar, sendo a intensidade luminosa associada à lua cheia 60 *dB* abaixo da intensidade solar de um dia ensolarado (ver subseção 2.2.3.2), nos horários antes do nascer do sol e após o por do sol observamos apenas contagens de escuro dos detectores, variando aleatoriamente entre 130 Hz e 135 Hz. Entre o nascer e o por do sol, nota-se um aumento nas contagens para algo entre 140 Hz e 145 Hz, o que corresponde a um aumento de $\approx 7,5\%$ no nível de ruído no sistema, com pico em aproximadamente 165 Hz ($\approx 25\%$ de incremento no ruído) próximo às 16 horas. Ou seja, se a QBER média para transmissões realizadas à noite é da ordem de 3,6%, considerando que os erros ocasionados por contraste imperfeito de polarização não sejam alterados, a média da QBER não será maior que $\approx 3,64\%$ durante o dia, com pico inferior a $\approx 3,72\%$, devido à influência da luz solar. Mas, na realidade,

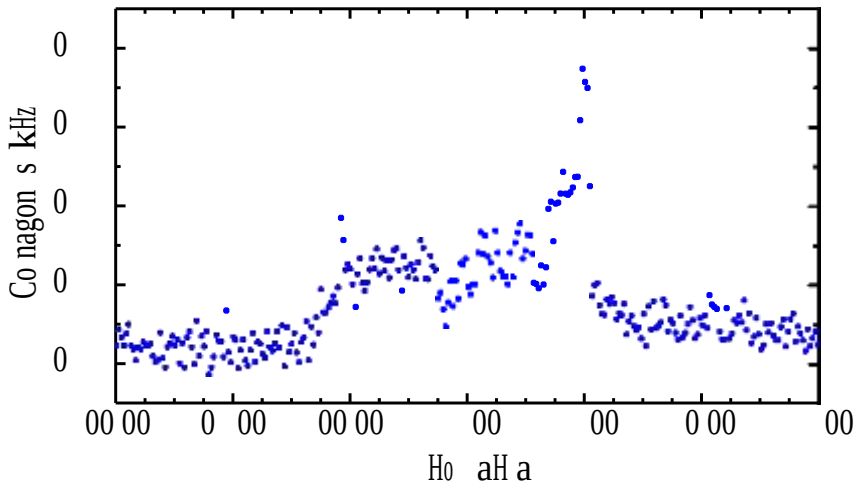


Figura 5.28: Medições da contagem de fótons para a luz do sol ao longo de 24 horas, com filtro óptico, em dia ensolarado.

estes valores máximos nunca serão atingidos, pois nem todos os fótons solares captados serão geradores de bits errados na chave de Bob. De fato, a influência solar será muito menor do que esta. Vejamos.

A luz do sol detectada, por ser na maior parte captada após a reflexão em corpos presentes no entorno do enlace, apresenta polarização predominantemente horizontal. Seguindo esta linha de pensamento, e, mais uma vez sendo conservador e facilitando o raciocínio, admitindo que toda a luz do sol captada esteja na polarização horizontal, são quatro cenários majoritariamente possíveis:

– (a) o fóton solar incide no detector $|H)$ juntamente com um fóton transmitido;
– (b) o fóton solar incide no detector $|H)$ ao mesmo tempo que um fóton transmitido incide no detector $|V)$;
– (c) o fóton solar incide no detector $|H)$ sem que haja fóton transmitido detectado na mesma janela, em um momento em que havia sido transmitido um qubit $|H)$; ou
– (d)o fóton solar incide no detector $|H)$ sem que haja fóton transmitido detectado na mesma janela, em um momento em que havia sido transmitido um qubit $|V)$.

Como as sequências de bits enviadas são aleatórias, na média, metade dos bits são "0"s e metade são "1"s, logo, os itens (a) e (b) ocorrem, cada um, na metade das vezes em que ocorre alguma detecção conjunta entre fóton solar e fóton transmitido. Fazendo uso das médias obtidas na seção 5.4, verificamos que obtemos alguma detecção em $\approx 3,03\%$ das janelas de detecção abertas,

logo, estatisticamente, o caso (a) ocorrerá em 1,51% das vezes em que um fóton solar for detectado e o caso (b) também em 1,51% das vezes. Em ≈ 96,97% das vezes não há qualquer detecção, logo, os casos (c) e (d) ocorrerão em 48,49% das vezes, cada um.

A ocorrência de (a) não tem influência nenhuma no estabelecimento da chave, pois o SPAD já indicaria uma contagem certa devida ao fóton transmitido. A ocorrência de (b) gera uma janela desperdiçada por detecção nos dois SPAD ao mesmo tempo, logo, não tem influência na QBER, mas somente na taxa de transmissão de bits. Como só ocorre em 1,51% das vezes em que um fóton originado da luz solar for detectado, isto representa um incremento médio de $0,0151 \times (140 - 130) \approx 0,15$ *bps*, o que podemos desprezar se comparado às taxas médias obtidas da ordem de 30 *kbps*. A ocorrência de (c) gera um bit correto na sequência de Bob em comparação à sequência de Alice. A ocorrência de (d) gera um bit errado na sequência de Bob em comparação à sequência de Alice. Tanto a ocorrência de (c) quanto de (d) ocasionam um aumento na taxa de transmissão de bits, pois inserem uma detecção em uma janela que de outra forma seria vazia.

Como (c) e (d) têm a mesma probabilidade de ocorrer, eles inserem uma média de 50% de erros na chave dentro das $0,9697 \times (140 - 130) \approx 9,7$ janelas de detecção por segundo. Mais uma vez comparando com a QBER obtida experimentalmente em laboratório e fazendo a média ponderada de 3,6% de erros em ≈ 30330 *bits*, com 50% de erros em ≈ 9,7 *bits*, obtemos $(0,036 \times 30330 + 0,5 \times 9,7)/(30330 + 9,7) \approx 3,615\%$, o que essencialmente resulta em uma QBER média aumentada em apenas 0,15 pontos percentuais durante o dia, se comparada à QBER obtida em laboratório e à QBER teórica correspondente ao período noturno. Fazendo a mesma conta para o pico das 16 horas, a QBER afetada pelo sol será de

$$(0,036 \times 30330 + 0,5 \times 33,94)/(30330 + 33,94) \approx 3,652\% \qquad (5\text{-}1)$$

Podemos concluir, então, que a rede de Bragg é eficaz como filtro da luz solar, uma vez que as variações teóricas da QBER devido a esta fonte de ruídos é pequena e encontra-se dentro da faixa de oscilações obtida no experimento back-to-back realizado dentro do laboratório. Portanto, estamos prontos para o estabelecimento da comunicação via enlace ao ar livre para constatação experimental da teoria aqui discutida.

5.5.2

Estabelecimento das Chaves e Análise dos Resultados

Em primeiro lugar, não podemos esquecer que, para o experimento realizado ao ar livre, nos telhados, foi necessária a introdução do Pol Tracker, do WDM, do combinador óptico (na verdade, um *BS 50/50*, que introduz no mínimo 3, 0 *dB* de perda) e de 128 *m* de fibra óptica para levar a luz do laser de dentro do laboratório para o telhado. O esquema deste setup é repetido aqui na figura 5.29 para facilitar a visualização. Estes novos dispositivos somados introduzem uma perda de 22, 6 *dB*. Como a atenução no VOA foi ajustada para somente 24, 1 *dB* (quando o ajuste anterior atenuava 58, 9 *dB*) os 69, 0 *dB* de atenuação existentes no setup utilizado no laboratório passam a ter um valor total de 56, 8 *dB* no transmissor. A grande atenuação *no transmissor* não tem efeito deletério no experimento, uma vez que estamos interessados no estudo da energia sendo acoplada da fibra óptica ao espaço livre e se propagando pela atmosfera, logo, podemos ajustar a potência do laser ou a atenuação no VOA para compensar estas perdas e considerar que, em um sistema com poucas perdas, usaríamos menor potência de laser. O resultado do estudo não será afetado.

No receptor não foram necessárias mudanças, pois a distância entre o canhão receptor e seus equipamentos associados no local de sua instalação é a mesma de dentro do laboratório.

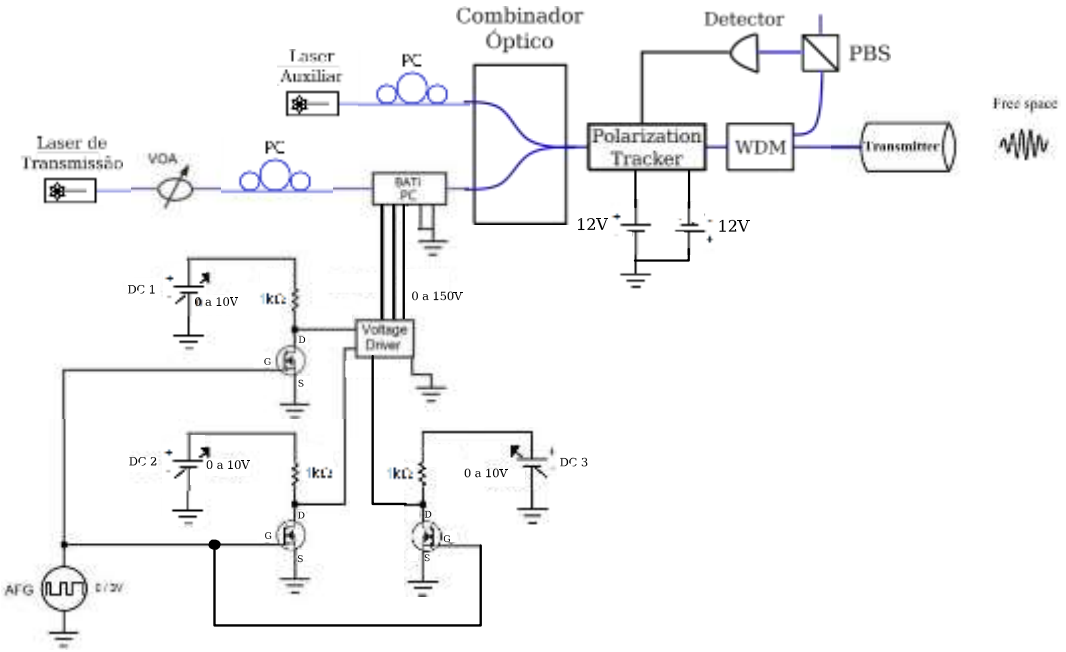


Figura 5.29: Setup experimental defintivo do transmissor.

No transmissor, a luz gerada pelo laser é emitida pela extremidade aberta da fibra óptica, ocupando um cone equivalente a sua abertura numérica. Observando a figura 5.30, percebe-se claramente que o modo gerado não é

o modo $TEM_{(0,0)}$, mas sim um modo de ordem mais alta, um padrão de círculos iluminados intercalados com círculos escuros, em torno do centro mais claro, onde está concentrada a maior parte da energia luminosa. O padrão observado não é consistente com a teoria de feixes gaussianos, que prevê que aproximadamente 86% da energia luminosa está contida em um círculo de raio $W(z)$, enquanto 99% da energia está contida em um círculo de raio $1,5W(z)$, o que pode claramente ser visto na foto que não é o caso. Este é um efeito combinado do próprio laser, que não é um laser preparado especificamente para laboratórios experimentais e já não emite perfeitamente no modo ($TEM_{(00)}$), com o fato de ele passar por uma fibra multimodo até ser lançado pelo canhão transmissor. O diâmetro do feixe para o laser verde foi medido no local do receptor durante o procedimento de alinhamento, tendo sido obtido um valor aproximado de 11 *cm* para a região onde há grande concentração da energia luminosa.

Figura 5.30: Padrão de intensidade luminosa obtido no receptor com a utilização do laser verde de comprimento de onda de 532 *nm*.

Para o laser infravermelho, provavelmente obtemos modos propagantes diferentes e com divergência diferente, mas podemos estimar a perda causada pela divergência ao compararmos as medidas obtidas em configuração back-to-back com as obtidas ao ar livre. Como mencionado, para obtermos na saída da fibra óptica do canhão receptor, em medições durante o por do sol, a mesma medição de potência em back-to-back e ao ar livre, foi necessário ajustar o atenuador no transmissor para atenuar $34,8\ dB$ a menos $(58,9 - 24,1)$, na configuração ao ar livre e considerando que a inserção dos dispositivos de manutenção de polarização somados introduzem uma perda de $22,6\ dB$,

podemos dizer que as perdas associadas à divergência do feixe somadas às perdas associadas ao espaço livre correspondem a $\approx 12,2\ dB$. Ao calcularmos, mais à frente, as perdas associadas ao espaço livre por absorção e espalhamento, poderemos estimar qual parte dos $12,2\ dB$ da perda se deve à divergência. Em um sistema comercial, um conjunto de lentes específicas para este sistema poderia facilmente ser projetado, de modo que o feixe tenha divergência tão pequena quanto se queira, para que o raio do feixe, $W(z)$, chegue ao receptor menor que o da lente dele, o que faria com que não houvessem perdas por divergência do feixe, melhorando o rendimento do sistema.

Devido à necessidade de realização de manutenção no canhão transceptor, com fabricação de uma nova peça para ajuste de foco para substituir uma danificada, e a presença de ventos de moderados a fortes em alguns dias[5], não houve tempo disponível para realizar medições em vários dias diferentes. Porém, os três dias disponíveis foram bastante aproveitados, tendo gerado, no total, 104 transmissões válidas. Estas transmissões foram realizadas na primeira quinzena de dezembro, época em que o sol se encontra sobre o hemisfério sul, já próximo ao solstício de verão, quando a incidência de luz solar na cidade do Rio de Janeiro é maior. Nos três dias o céu estava nublado e, segundo o *website* do *weather channel* (www.weather.com), a visibilidade era de 16 *km* nos horários das realizações das transmissões. A tabela 5.2 mostra os outros parâmetros das condições climáticas nos momentos dos experimentos.

Tabela 5.2: Condições climáticas nos dias das realizações de transmissões. Fonte: *www.weather.com*.

Horário	Presença de névoa	Vento Médio	Direção	Rajadas	Umidade Relativa
À tarde	neblina leve	9 km/h	SE	15 km/h	83%
Por do sol	neblina leve	9 km/h	SO	17 km/h	86%
À noite	sem neblina	7 km/h	SE	11 km/h	87%

Assim como no caso back-to-back, as transmissões foram realizadas com várias durações diferentes, a fim de verificar o efeito da falta de sincronismo de clock entre o transmissor e o receptor. A figura 5.31 mostra o resultado para transmissões durante o dia e vemos que o melhor tempo de transmissão é de 3 segundos, a fim de manter a QBER média o mais baixa possível, sem também reduzir a quantidade de bits nas chaves a um nível ineficiente. Mesmo para 10 segundos, que gera uma QBER média próxima de 6,5%, seria possível estabelecer uma chave secreta, uma vez que a QBER está bem abaixo do limite de 12%.

[5] A influência do vento será discutida mais adiante nesta seção.

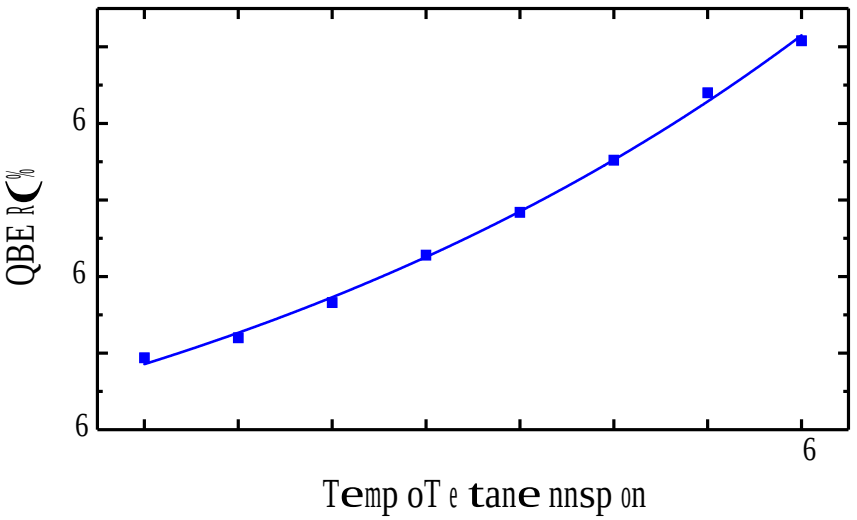


Figura 5.31: QBER em função do tempo de transmissão, para transmissões ao ar livre.

Para a transmissão durante o dia em "rajadas" de 3 segundos, a taxa média de bits para chaves criptográficas é de 26900 *bps*. Observe que já é possível realizar um cálculo preliminar da atenuação no canal. Nos experimentos em back-to-back, a taxa obtida foi de 30330 *bps*, logo, a influência do meio externo reduziu a taxa em ≈ 11, 3%. Para as transmissões durante o por do sol e durante a noite, foram obtidas, respectivamente, taxas de 27000 *bps* e 29170 *bps*, que representam atenuações de ≈ 11% e ≈ 3, 8%. Podemos ver na tabela 5.3 os parâmetros monitorados para as três condições do experimento. Para todos os efeitos, os valores das taxas de bits, tamanho das chaves, janelas úteis e janelas vazias para as medições à tarde e próximo ao por do sol são semelhantes o suficiente para que possamos tratá-las como valores iguais.

Tabela 5.3: Parâmetros obtidos para as transmissões de qubits com o enlace nos telhados em 3 condições de tempo diferentes.

Condição	QBER (%)	Taxa de bits (bps)	Tamanho das chaves (bits)	Janelas Úteis (%)	Janelas Vazias (%)	Janelas com dupla detecção (%)
À tarde	4,47	26900	80700	2,69	97,31	0,0048
Por do sol	3,86	27000	81000	2,70	97,30	0,0026
À noite	6,20	29170	87510	2,92	97,07	0,0022

QBER

Vamos analisar em primeiro lugar a QBER. O primeiro fato a chamar nossa atenção é que a QBER foi significativamente maior do que nos experimentos realizados dentro do laboratório (sem a influência de fatores externos). A tabela 2.2 nos diz que a intensidade de dias nublados é uma ordem de grandeza abaixo da intensidade para dias de sol. Somado a isto, vimos na figura 5.28

que a contribuição da luz solar em dias ensolarados, quando filtrado pela rede de Bragg tem um pico de apenas 30 contagens por segundo acima da contagem de escuro, portanto, em dias nublados, essa contribuição deverá ser da ordem de 3 contagens por segundo. A equação (5-1) nos dá um valor teórico para o efeito destas 30 contagens por segundo (dia ensolarado) na QBER no horário em que a influência da luz solar tem um pico: 0,052 pontos percentuais. Em dias nublados, a expectativa é que a influência da luz solar na QBER seja $\approx 0,0052$ pontos percentuais (uma ordem de grandeza a menos). Ademais, a maior QBER foi obtida à noite, quando o ruído gerado por iluminação é da ordem de 50 *dB* abaixo de um dia nublado. Então, podemos concluir que o aumento da QBER não foi causado por ruído gerado pela luz solar. Tão pouco o ruído de escuro dos SPAD pode ter sido responsável por isso, uma vez que todas as suas configurações se mantiveram inalteradas e eles estavam localizados em sala refrigerada, com temperatura controlada.

Resta um fator, entretanto, que certamente foi o causador deste aumento na QBER: *contraste imperfeito nas polarizações*. E o vento tem papel fundamental nesta imperfeição. Ao se propagar em espaço livre, o fóton, em princípio, não sofre alteração de sua polarização. Porém, entre o Pol Tracker e o canhão transmissor, os fótons percorrem uma fibra óptica e, dentro da fibra, o fóton tem sua polarização alterada. Mas este fato, por si só, não é prejudicial ao sistema, uma vez que as variações espaciais de polarização se mantenham estáveis no tempo. Assim, independente de qual polarização esteja efetivamente saindo do canhão transceptor, ela sempre será a mesma captada no receptor, podendo ser alinhada com os eixos do PBS durante a calibração do sistema.

O problema ocorre quando a polarização varia no tempo, o que acontece sempre que a fibra se mexe. Daí a influência do vento ser tão significativa. Como este sistema é experimental, e não um sistema comercial, os equipamentos não estão todos encapsulados em um só invólucro e, desta forma, os poucos metros de fibra óptica expostos ao vento já são suficientes para fazer a polarização dos fótons oscilar com o tempo. E ela oscila muitas vezes por segundo, a depender da frequência funamental do vento. É muito fácil perceber a presença do vento durante o procedimento de calibração. Como já foi dito anteriormente, a contagem de escuro dos SPAD utilizados é da ordem de 135 Hz. Assim sendo, um SPAD deveria apresentar a contagem de 135 Hz quando enviado apenas o qubit ortogonal ao dele se fosse obtida uma calibração perfeita. Durante as calibrações feitas em back-to-back, foi conseguida uma contagem de escuro de ≈ 200 Hz. Já para as transmissões ao ar livre, essas contagens não foram inferiores a 800 Hz, 400 Hz e 2 kHz, para as transmissões à tarde, ao por do sol e à noite, respectivamente. À noite, foi necessário refazer a calibração a

cada cinco medições e, mesmo assim, várias medições foram descartadas por terem apresentado QBER acima de 12% (duas delas inclusive acima de 30%).

A relação da QBER com o vento, indiretamente, através do contraste de polarização, pode ser confirmada qualitativamente se verificarmos que a menor QBER obtida foi conseguida no dia que o vento estava bloqueado pelo morro e, portanto, no local da instalação do transmissor não havia vento (constatação *in loco*). Aparentemente, olhando a tabela 5.2, parece que havia mais vento à tarde do que à noite e, portanto, a QBER obtida à tarde deveria ser maior. Contudo, as transmissões realizadas à tarde só foram conseguidas em um momento em que o vento amansou por alguns minutos, após mais de uma hora de tentativas frustradas pelo vento. Este fato se confirma pelas contagens obtidas nos SPAD durante a calibração.

Janelas com dupla indicação

Passemos, então, às janelas de detecção que apresentaram dupla indicação, ou seja, que o SPAD-0 e o SPAD-1 indicaram a detecção de um fóton ao mesmo tempo. Como discutido anteriormente, vimos que o maior influenciador deste fenômeno é a própria contagem de escuro do detector, quando ela ocorre simultaneamente à detecção de um fóton real pelo outro detector. Na seção 5.4.1 foi dito que, para a configuração back-to-back, todos os casos experimentais apresentaram taxa de janelas com dupla detecção menor que 0,004%. A média obtida para aquela configuração foi de 0,0023%. Os dados da tabela 5.3 nos mostram que, além da contagem de escuro, os ruídos do canal também têm influência nestes números. Todavia, como esperado, esta influência é muito pequena para afetar o desempenho do sistema.

Já foi discutido neste trabalho que o maior gerador de ruídos para sistemas de FSOC em infravermelho próximo é o sol. Quando um fóton solar (gerado pelo sol) é detectado por um SPAD na mesma janela temporal de detecção em que o outro SPAD detecta um fóton transmitido, há uma indicação de dupla detecção. Já vimos também que a rede de Bragg funciona como um excelente filtro para este fenômeno e este fato se reflete nos índices apresentados na tabela. As taxas durante o por do sol e à noite são de valor muito próximo aos obtidos dentro do laboratório, enquanto à tarde, a taxa é aproximadamente o dobro deste valor. Ainda que seja o dobro, de fato este valor é tão pequeno (variação da ordem de 0,0025 pontos percentuais) que não oferece degradação significativa da taxa de transmissão de bits efetiva do sistema.

Perdas no enlace

Procederemos agora a uma análise única para os demais resultados constantes da tabela 5.3, pois todos eles reagem às mesmas influências. Mantendo-se contantes a potência e o tempo de transmissão, temos que a taxa de bits, o tamanho obtido para a chave, a porcentagem de janelas úteis e a porcentagem de janelas vazias nada mais são que quatro formas de enxergar a mesma coisa. Quanto menos perdas no canal, maiores as três primeiras e menor a quarta, e vice-versa.

O principal fator causador de janelas vazias é o próprio SPAD, que tem eficiência de apenas 25% (perda de 6 *dB*) e ainda é responsável por perdas de mais 23 *dB* devido ao seu *duty cycle* de 1/200. Somando todas as perdas apresentadas até aqui, temos:

- Laser ajustado para 0 dBm;
- Atenuação de 56, 8 *dB* no transmissor;
- Atenuação de 12, 2 *dB* no espaço livre mais divergência do feixe;
- Atenuação de 17, 0 *dB* no receptor;
- Atenuação de 29 *dB* no SPAD;
- Potência teoricamente detectada pelo SPAD, somando-se todas as atenuações acima, de ≈ -115 dBm.

Ora, podemos calcular a quantos fótons por segundo equivale esta potência.

$$P = 10^{(-115/10)}/1000 \approx 3,1623 \times 10^{-15} W \qquad (5\text{-}2)$$

Mas é sabido que $P = (n.h.c)/\lambda$, logo:

$$n = \frac{3,1623 \times 10^{-15} \times 1,55 \times 10^{-6}}{6,63 \times 10^{-34} \times 3 \times 10^{8}}$$

$$n \approx 24643,36 \text{ detecções de fótons/s} \qquad (5\text{-}3)$$

Ora, mas com um clock de 1 MHz, 24643, 36 detecções por segundo representam 2, 46% de janelas com detecções e o valor obtido experimentalmente foi de 2, 70%, próximos o suficiente para validarem-se. Se utilizarmos os valores experimentais de 2, 70% de janelas válidas para as medidas de dia e 2, 92% de janelas válidas para as medidas à noite, obtemos atenuações experimentais

totais de 114, 60 *dB* (dia) e 114, 26 *dB* (noite). As diferenças entre as atenuações experimentais obtidas ao ar livre e em back-to-back, já compensados os reajustes realizados no VOA e as perdas inseridas pelo Pol Tracker e seus acessórios são de 11, 80 *dB* (dia) e 11, 46 *dB* (noite) e só podem estar localizadas no espaço livre, pois todo o restante permaneceu inalterado. Estes valores são mais precisos que o valor teórico de 12, 2% obtido anteriormente através de cálculo preliminar. Vejamos, então, como estão distribuídas estas perdas entre os canhões.

Foi discutido no capítulo 2 que as fontes de perdas nos sistemas de FSO são o espalhamento e a absorção dos fótons por elementos da atmosfera. A absorção, por sua vez, na janela atmosférica de transmissão sendo utilizada (1550 *nm*), é causada principalmente por aerossóis urbanos e moléculas de água e de CO_2 presentes na atmosfera, como pode ser visto nos gráficos das figuras 2.12 a 2.15. Os gráficos citados mostram as características de absorção da atmosfera, como simuladas em software, para situações de visibilidade média de 5 *km*. No nosso caso, a visibilidade média estimada é de 16 *km*, mas podemos fazer uma aproximação a fim de entender os fenômenos que ocorrem com o nosso sistema.

A figura 2.14 mostra uma transmissão para o CO_2 com valor 1 para a nossa janela de transmissão, o que significa que o dióxido de carbono não absorve luz no comprimento de onda de 1550 *nm*. A figura 2.13 nos dá um valor suficientemente próximo de 1 para podermos aproximar para 1. Portanto, podemos considerar que toda a absorção está sendo causada pelos aerossóis. O gráfico apresentado na figura 2.15 mostra que a transmissão para os aerossóis é em torno de 0, 8, o que equivale a dizer que 20% dos fótons serão absorvidos pelos aerossóis. Mas a visibilidade nos momentos de nossas medições era da ordem de três vezes maior que a da simulação mostrada no gráfico. Ademais, aquele gráfico não especifica uma relação com o comprimento do enlace. Da referência [67] podemos extrair a equação para atenuação por aerossóis urbanos por quilômetro de enlace, para uma visibilidade de 20 *km* (mais próximo do nosso caso):

$$T_h = e^{-\beta_p(h)d} \tag{5-4}$$

Onde T_h é a transmissão atmosférica para a altitude h da localização do enlace, d é a distância entre o transmissor e o receptor e $\beta_p(h)$ é o coeficiente de atenuação espectral para a altitude h da localização do enlace. Nosso enlace está situado na cidade do Rio de Janeiro, ao nível do mar, logo, $h \approx 0$. A referência fornece os valores $\beta_p(0) = 0,108\ km^{-1}$ para $\lambda = 1,26\ \mu m$ e $\beta_p(0) = 0,098\ km^{-1}$ para $\lambda = 1,67\ \mu m$. Podemos, com tranquilidade, usar o

valor de $\beta_p(0) = 0,10\ km^{-1}$ para o nosso $\lambda = 1,55\ \mu m$. Inserindo os valores referentes ao nosso enlace na equação (5-4):

$$T_0 = e^{-0,1\times0,16} \approx 0,9841 \quad (5\text{-}5)$$

O que equivale a uma atenuação de apenas $0,0695\ dB$, ou $\approx 0,07\ dB$ causada por absorção na atmosfera. Como a nossa transmissão noturna é que foi realizada com céu limpo e não temos uma fórmula disponível para calcular a absorção em dias de neblina leve, vamos primeiramente utilizar a noturna como referência.

Quanto ao espalhamento, vimos que, dentre as formas possíveis, o espalhamento de Mie causado pelo nevoeiro é a principal fonte de atenuação do feixe em FSO e que esse efeito é acentuado geometricamente à medida que a distância é aumentada. A turbulência terá efeito mínimo de espalhamento de fótons neste experimento, uma vez que ele foi realizado em dias com temperatura amena, com potências baixas e todos os cuidados citados na subseção 2.2.1.5 foram tomados, à exceção da instalação na beirada do prédio.

Da tabela 2.1, podemos estimar o espalhamento devido à neblina leve para visibilidade média de $16\ km$. Tomando os valores da tabela para neblina leve (5, 9 e $10\ km$), podemos interpolar para $16\ km$ e obtemos uma atenuação aproximada de $0,32\ dB/km$, o que, para os nossos $160\ m$ de distância, é equivalente a $0,0512\ dB$ de atenuação para as medidas à tarde. Ainda que a variação da atenuação não seja exatamente linear com a visibilidade, a distância utilizada neste trabalho é pequena e o valor de atenuação também pequeno, logo, a diferença da não-linearidade será menor que o próprio arredondamento da conta realizada. Fazendo extrapolação semelhante no caso de céu limpo ($18,1$ e $20\ km$) para os $16\ km$ de visibilidade, obtemos uma atenuação de $0,26\ dB/km$, que para a distância de $160\ m$ correponde a atenuar $0,0416\ dB$.

Havíamos estimado que o canal é responsável por aproximadamente $11,46\ dB$ das perdas do sistema para a transmissão noturna. Ora, se a absorção é responsável pela atenuação de $0,07\ dB$ e o espalhamento por $0,04\ dB$, o que resta, $11,35\ dB$, é resultado do que é perdido por divergência do feixe e nem atinge a lente do receptor. Ou seja, $92,67\%$ da energia que sai do canhão transmissor é perdida porque nem atinge a lente do receptor, por causa da divergência do feixe.

Como a divergência do feixe não varia, podemos, agora, utilizar o valor obtido para estimar a absorção atmosférica em condição de neblina leve, de dia. A divergência do feixe é responsável por $11,35\ dB$ e a perda por espalhamento calculada é de $0,05\ dB$ para esta condição. A atenuação total obtida para

espaço livre nesta situção foi de 11, 8 *dB*, portanto, a absorção é responsável por 0, 4 *dB*. A tabela 5.4 mostra um resumo dos valores experimentais das perdas em cada seção do sistema.

Tabela 5.4: Resumo dos valores das perdas obtidos experimentalmente para cada seção do sistema.

Elemento	Dia	Noite
Ajuste do laser	0 dBm	0dBm
Atenuação no transmissor	56,8 dB	56,8 dB
Absorção na atmosfera	0,4 dB	0,07 dB
Espalhamento na atmosfera	0,05 dB	0,04 dB
Divergência do feixe	11,35 dB	11,35 dB
Atenuação no receptor	17,0 dB	17,0 dB
Atenuação no SPAD	29,0 dB	29,0 dB
Potência detectada	-114,60 dBm	-114,26 dBm
Janelas aproveitadas	2, 70%	2, 92%

Análise da possibilidade de uso do sistema por embarcações

O estudo realizado neste trabalho tem como um dos objetivos a análise para aplicação do sistema de FSO para distribuição de chaves quânticas em enlaces entre embarcações e estações costeiras, como o próprio título do trabalho estabelece. A cidade do Rio de Janeiro e, em particular, o bairro em que os experimentos foram realizados, é uma localidade costeira e apresenta características muito semelhantes ao que seria obtido em uma comunicação realizada entre uma embarcação e uma estação costeira, inclusive apresentando o mesmo tipo de neblina [26]. Uma diferença fundamental é a distância do enlace realizado, pois 160 *m* é uma distância muito pequena para as características de navegação costeira, que é definida como aquela realizada a uma distância de até 20 milhas náuticas (37040 *m*) da linha de base da costa, o que necessitaria um enlongamento da ordem de 230 vezes no enlace utilizado neste trabalho, o que pode não ser exequível. Já para o estabelecimento de link entre embarcações navegando em comboio, que costumam navegar a distâncias bem menores entre si (500 jardas ou 457 metros em média, e máxima de 1000 jardas ou 914 metros), precisaríamos aumentar o enlace em apenas 5, 7 vezes. Mas então, qual a distância máxima aplicável a este projeto?

A resposta é: depende. Certamente o ruído do canal é um limitador, pois, quanto maior a distância, mais suscetível a ruídos o enlace está e maior será a QBER, que, como já vimos, não pode ser maior que 12%. Mas também as

perdas são um limitador, na medida em que existe uma taxa de transmissão mínima aceitável. E pode ser que o limitador determinante seja este. A taxa mínima aceitável pode ser diferente para cada aplicação. Neste trabalho foram conseguidas taxas de transmissão da ordem de 27 *kbps*, porém, há experimentos em que são aceitas taxas da ordem de até 0,1 a 2 *kbps* [68].

Se decidirmos que taxas da ordem de 1 *kbps* são aceitáveis, significa que obteremos 0,1% de janelas com detecção e, portanto, poderemos ter perda total no sistema de 128,92 *dB*, ou perda adicional de 14,66 *dB* com relação ao enlace experimental. Considerando, ainda , que a implementação do verdadeiro protocolo BB84, com duas bases não-ortogonais sendo alternadas aleatoriamente por Alice e Bob, gera chaves 50% mais curtas (no pior caso) devido aos momentos em que Alice e Bob realizaram medidas em bases diferentes, isto equivale a uma perda de 3 *dB*, logo, a perda adicional permitida, com relação ao que obtivemos experimentalmente, associada ao espaço livre é de 11,66 *dB*. É importante notar que as perdas no sistema transmissor e no sistema receptor são independentes da distância em que se estabelece o link, logo, devemos analisar somente a diferença das perdas associadas ao canal óptico para o cálculo da distância máxima do enlace.

Para que a variável limitante esteja relacionada somente à atmosfera, vamos considerar que podemos projetar canhões transceptores e lentes específicas para a distância máxima que será aqui calculada, de forma que a perda por divergência do feixe se mantenha em, no máximo, os mesmos 11,35 *dB* calculados aqui.

Já vimos anteriormente que as perdas atmosféricas são devidas principalmente ao espalhamento de Mie e à absorção por aerossóis urbanos. Vamos aqui considerar o caso dos navios se comunicando com estações costeiras nas condições de céu limpo, para as quais temos a fórmula de Elterman para a absorção. Sendo conservador, vamos considerar que a distância do navio à costa é suficientemente pequena para que a distribuição de aerossóis urbanos ocupe todo o trajeto de comunicação.

Utilizando a equação (5-4) para a absorção e a atenuação de 0,26 *dB/km* obtida pela interpolação dos valores da tabela 2.1, podemos escrever:

$$-11,66 = 10\log(e^{-0,1d_{max}}) - 0,26d_{max} \qquad (5\text{-}6)$$

Logo, $d_{max} \approx 16,8\ km$, o que é compatível com o experimento citado ([68]). Portanto, podemos concluir que, desde que permitidas baixas taxas de transmissão de bits, este experimento e os cálculos teóricos associados validam a possibilidade do uso de FSOC para QKD tanto de uma embarcação para outra quanto entre embarcações e estações costeiras, ainda que, neste último

caso, não seja possível chegar ao limite definido pela autoridade marítima como navegação costeira.

Quanto à QBER associada a esta nova distância, da ordem de dezena de quilômetros, seria necessário fazer um estudo mais aprofundado, mas não há razões para crer que a taxa fique maior que 12% (nem próxima disso) devido aos ruídos do canal. Os resultados obtidos para a QBER com um enlace de 1, 60 *m* em local controlado e com um enlace cem vezes mais longo, de 160 *m*, e sujeito às intempéries são muito próximos e a pouca diferença entre eles é atribuída majoritariamente à imperfeição de contraste de polarização, que é um problema de calibração, não do meio. Caso o sistema seja todo encapsulado, tanto no transmissor quanto no receptor, desde o canhão transceptor até o último elemento, este problema tende a ser minimizado e as QBER tendem a ser semelhantes. A distância máxima teórica calculada é também da ordem de cem vezes maior que nosso enlace experimental ao ar livre, logo, diferenças em escala são esperadas.

A grande dificuldade esperada para um enlace tão distante é o alinhamento dos canhões. Tanto o alinhamento inicial quanto a manutenção deste alinhamento ao longo do tempo, principalmente quando o enlace envolve embarcações, que estão sujeitas ao balanço devido às oscilações das ondas do mar. Uma forma possível de conseguir manter o alinhamento seria o uso de um laser paralelo, em um comprimento de onda lateral e de maior abertura, no transmissor e um detector por quadrantes no receptor, com um sistema eletrônico de controle para ajuste da posição do canhão em função da diferença de potência detectada em cada quadrante, conforme sugerido por Ozek em [69] e por Harres em [70]. Seria possível até utilizar o mesmo laser para controle do alinhamento dos canhões e para a implementação do clock sugerido no *caput* deste capítulo.

Não há ganho de informação em se repetirem aqui as aplicações das chaves criptográficas em textos e em imagens, como foi feito na subseção 5.4.2, uma vez que as QBER obtidas nesta seção são suficientemente parecidas com aquelas para que haja alguma diferença visual significativa nas imagens apresentadas.

6
Conclusões

Com a relativa proximidade do desenvolvimento de computadores quânticos e a possibilidade cada vez menos remota do desenvolvimento de chips com algoritmos clássicos capazes de inviabilizar as formas de criptografia comumente utilizadas hoje em dia, o estudo e desenvolvimento da criptografia quântica se torna imperativo, pois a segurança da informação é garantida pelas leis da física, em oposição ao que temos hoje, garantida apenas pela dificuldade de quebra do código criptográfico ou pelo tempo que seria necessário para esta quebra.

Ao mesmo tempo, vêm sendo desenvolvidos sistemas de comunicações ópticas em espaço livre a distâncias cada vez maiores, inclusive para comunicações espaço-Terra, com a iminente instalação de um sistema de comunicações no infravermelho entre a estação espacial internacional e a superfície terrestre. O desenvolvimento de computadores quânticos certamente requererá a criação de redes quânticas de computadores, que serão compostas parte em fibra óptica e parte em espaço livre, formando sistemas híbridos, em que a energia luminosa será acoplada da fibra para o espaço livre e vice-versa.

Desta forma, congruem a necessidade do desenvolvimento de sistemas de comunicações quânticas para QKD, com o entendimento dos efeitos e o aprimoramento de seu uso em espaço livre e com o acoplamento deste meio de transmissão à fibra óptica, ao menos para tratamento dos sinais em computadores quânticos.

Neste trabalho foi apresentado um experimento de transmissão, entre dois indivíduos, de qubits codificados em polarização em um sistema híbrido fibra-óptica – espaço-livre com o objetivo de realizar uma prova de princípios da possibilidade de estabelecimento de links para QKD e também de realizar um estudo das características da atmosfera como meio de comunicação para a realização do QKD. Para isto, foram testadas várias configurações possíveis até que fosse escolhida a mais adequada e foram desenvolvidos um software para a comunicação da FPGA com os detectores e com o computador que armazena os dados coletados, um software para conciliação das chaves e um software para a comparação entre as chaves gerada e recebida e análise dos resultados. Foram também simuladas transmissões de mensagens de texto e

de imagens criptografadas com a chave compartilhada pertencente a Alice, e descriptografadas com a chave pertencente a Bob. Ficaram evidentes os erros obtidos nas mensagens descriptografadas, ainda que as imagens sejam perfeitamente compreensíveis e não haja perda de informação por Bob. Já as mensagens de texto ficaram ininteligíveis. Os experimentos com a configuração final foram realizados em duas situações diferentes, para fins de comparação de resultados.

A primeira, consistiu na transmissão dos qubits, codificados em polarização, entre dois indivíduos localizados a 1,60 *m* de distância (espaço livre), em ambiente isento de influências externas (ou, mais precisamente, com influência externa controlada) e o estabelecimento de chaves criptográficas compartilhadas entre os dois indivíduos. Desta forma, foi possível caracterizar o sistema. A segunda foi a transmissão equivalente, mas para uma distância de 160 *m* em espaço livre, em ambiente externo, sujeito às variações de temperatura, luminosidade solar, ventos, chuvas e neblinas. Uma seção de quatro metros da parte do sistema em fibra óptica também encontrava-se sujeita a estas mesmas intempéries. De posse dos resultados experimentais ficou comprovado que o esquema utilizado, na janela atmosférica de 1550 *nm*, é capaz de obter taxas de erro (QBER) da ordem de um terço do limite de 12% para garantir o segredo da chave criptográfica, ou seja, a segurança da informação. Foi demonstrado, ainda, que é possível realizar uma excelende filtragem da maior fonte de ruídos do espaço livre, o sol, de forma a obter uma influência menor que 0,005% nos resultados.

A distância máxima teórica, calculada a partir dos resultados experimentais, permite que embarcações em navegação costeira consigam estabelecer um link para QKD com estações em terra a uma distância de aproximadamente 40% da distância máxima definida para este tipo de navegação, desde que baixas taxas de bits sejam aceitas. Para as comunicações entre embarcações, a distância máxima teórica para o link excede em 15 vezes a distância máxima entre embarcações em comboio, o que significa que taxas de bits bem melhores podem ser obtidas.

Foram também citadas oportunidades para a melhoria do sistema, caso se queira transformá-lo de um sistema de prova de princípios em um sistema comercial, e que serão deixadas como trabalho futuro. O ponto mais importante é o projeto de um novo sistema de lentes para o canhão transmissor que gere um feixe menos divergente, de forma que não haja informação sendo perdida (e disponível para Eva) por não atingir a lente do receptor. Este seria um projeto simples de óptica (mas provavelmente demorado), cujas referências são abundantes.

Outra necessidade importantíssima é a melhoria do clock do transmissor, pois resultaria em uma proximidade maior da sequência de bits transmitida com uma sequência realmente aleatória. Como mencionado no *caput* do capítulo 5, poderiam ser utilizados em série vários controladores de polarização do tipo piezoelétricos (BATI) ou um controlador de resposta mais rápida, como o de niobato de lítio (EOSpace). A instalação de todo o sistema em uma caixa fechada para anular a influência do vento também facilita o controle de polarização.

Por último, a implementação de um laser em um comprimento de onda lateral poderia ser utilizada para realizar sincronismo de clock e permitir maiores tempos de transmissão e perfeita correlação entre as janelas de transmissão e detecção (ver *caput* do capítulo 5), bem como para estabelecimento e manutenção de alinhamento dos canhões transceptores entre si de forma automática, incluindo no receptor um detector por quadrantes e um sistema de controle (citado na subseção 5.5.2).

Referências bibliográficas

[1] G. P. Agrawal, *Fiber-Optic Communication Systems*, 3rd ed., ser. Wiley Series in Microwave and Optical Engineering. Hoboken, New Jersey: John Wiley and Sons, 2002.

[2] Airbus. (2019) Bartolomeo: New external payload platform on the international space station. Acessado: 04–10–2019. [Online]. Available: http://www.airbusdshouston.com/public/downloads/Bartolomeo_US_2019-04-18.pdf

[3] T. Kawahara. The easy route the easy way: new chip calculates the shortest distance in an instant. Acessado: 30–01–2020. [Online]. Available: https://www.tus.ac.jp/en/mediarelations/archive/20200123001.html

[4] M. Murgia and R. Waters. Google claims to have reached quantum supremacy. Acessado: 30–01–2020. [Online]. Available: https://www.ft.com/content/b9bb4e54-dbc1-11e9-8f9b-77216ebe1f17

[5] Army Materiel Commander, *Engineering design handbook: Infrared military systems. Part One.* Washington, D.C.: U.S. Army Materiel Command, 1971.

[6] G. Brassard, "Brief history of quantum cryptography: a personal perspective," in *Proceedings of IEEE Information Theory Workshop on Theory and Practice in Information-Theoretic Security*. IEEE, Oct 2005, pp. 19–23.

[7] C. H. Bennet, G. Brassard, S. Breidbart, and S. Wiesner, "Quantum cryptography, or unforgeable subway tokens," in *Advances in Cryptology: Proceedings of Crypto '82*. Plenum Press, Aug 1982, pp. 267–275.

[8] C. Bennett and G. Brassard, "Quantum cryptography: public-key distribution and coin tossing," in *Proceedings of IEEE International Conference on Computers Systems and Signal Processing*, Bangalore, India, Dec 1984, pp. 175–179.

[9] A. K. Ekert, "Quantum cryptography based on bell's theorem," *Physical review letters*, vol. 67, no. 6, p. 661, 1991.

[10] A. Rogalski, "History of infrared detectors," *Opto-Electronics Review*, vol. 20, no. 3, pp. 279–308, Sep 2012. [Online]. Available: https://doi.org/10.2478/s11772-012-0037-7

[11] NASA. Optical payload for lasercomm science. Acessado: 04–10–2019. [Online]. Available: https://www.nasa.gov/mission_pages/station/research/experiments/explorer/Investigation.html?#id=840

[12] Revista Época Negócios. (2014) Comunicação via laser mudará a internet. Acessado: 04–10–2019. [Online]. Available: https://epocanegocios.globo.com/Caminhos-para-o-futuro/Desenvolvimento/noticia/2014/07/comunicacao-laser-mudara-internet.html

[13] MagiQ Technologies. About MagiQ. Acessado: 29–12–2019. [Online]. Available: https://www.magiqtech.com/company/

[14] Austrian Institute of Technology. (2004) World premiere: Bank transfer via quantum cryptography based on entangled photons. Acessado: 04–10–2019. [Online]. Available: https://web.archive.org/web/20130309095431/http://www.secoqc.net/downloads/pressrelease/Banktransfer_english.pdf

[15] C. Elliott and H. Yeh, *DARPA Quantum Network Testbed: Final Technical Report*. Massachussetts: BBN Technologies, 2007.

[16] F. Jordans. Swiss call new vote encryption system unbreakable. Acessado: 29–12–2019. [Online]. Available: https://web.archive.org/web/20071209214958/http://www.technewsworld.com/story/59793.html

[17] S. Quantum. Swiss quantum. Acessado: 29–12–2019. [Online]. Available: https://web.archive.org/web/20150228080058/http://swissquantum.idquantique.com/

[18] M. Sasaki, M. Fujiwara, H. Ishizuka *et al.*, "Field test of quantum key distribution in the Tokyo QKD Network," *Opt. Express*, vol. 19, no. 11, pp. 10 387–10 409, May 2011.

[19] Clay Dillow para Fortune Magazine. (2013) Unbreakable encryption comes to the U.S. Acessado: 04–10–2019. [Online]. Available: https://fortune.com/2013/10/14/unbreakable-encryption-comes-to-the-u-s/

[20] Austrian Academy of Sciences. (2016) First quantum satellite successfully launched. Acessado: 04–10–2019. [Online]. Available: https://www.oeaw.ac.at/en/oeaw/press/public-relations-and-communications/pressefotos/first-quantum-satellite-successfully-launched/

[21] Mike Wall para Space.com. (2016) China launches pioneering 'hack-proof' quantum-communications satellite. Acessado: 04–10–2019. [Online]. Available: https://www.space.com/33760-china-launches-quantum-communications-satellite.html

[22] Inside Science. (2018) Is China the leader in quantum communications? Acessado: 04–10–2019. [Online]. Available: https://www.insidescience.org/news/china-leader-quantum-communications

[23] Amy Nordrum para IEEE Spectrum. (2017) China demonstrates quantum encryption by hosting a video call. Acessado: 04–10–2019. [Online]. Available: https://spectrum.ieee.org/tech-talk/telecom/security/china-successfully-demonstrates-quantum-encryption-by-hosting-a-video-call

[24] F. Mims, "The first century of lightwave communications," in *Fiber Optic Reprint Series – Volume 28 – Fiber Optics Primer*. Illinois: Information Gatekeepers, Inc, 1994, pp. 1 – 10.

[25] Agamemnon, *The Oresteia*, 2nd ed. Princeton, New Jersey: Penguin Books, 1979.

[26] C. P. Colvero, "Análise experimental de sistemas de comunicações ópticas no espaço livre em diferentes comprimentos de onda," Ph.D. dissertation, Pontifícia Universidade Católica do Rio de Janeiro, Departamento de Engenharia Elétrica, Curso de Pós-Graduação em Engenharia Elétrica, Rio de Janeiro, 2005.

[27] B. E. A. Saleh and M. C. Teich, *Fundamentals of Photonics*, 2nd ed., ser. Wiley Series in Pure and Applied Optics. Hoboken, New Jersey: John Wiley and Sons, 2007.

[28] B. P. Lathi, *Modern Digital And Analog Communications Systems*, 3rd ed., ser. The Oxford Series in Electrical and Computer Engineering. Oxford University Press, USA, 1998.

[29] F. Calliari, "Automatic high-dynamic and high-resolution photon counting otdr for optical fiber network monitoring," Master's thesis, PUC-Rio, Rio de Janeiro – RJ, 2017.

[30] H. Willebrand and B. S. Ghuman, *Free space optics: enabling optical connectivity in today's networks*, 1st ed. Indiana, Indianapolis: SAMS publishing, 2002.

[31] G. P. Temporão, "Contagem de fótons no infravermelho próximo e médio via conversão de frequências aplicada a comunicações quânticas," Ph.D. dissertation, Pontifícia Universidade Católica do Rio de Janeiro, Departamento de Engenharia Elétrica, Curso de Pós-Graduação em Engenharia Elétrica, Rio de Janeiro, 2007.

[32] S. Karp, R. Gagliardi, S. Moran, and L. Stotts, *Optical Channels: Fibers, Clouds, Water, and the Atmosphere*, 1st ed., ser. Applications of Communications Theory. New York, NY: Springer Science+Business Media, LLC, 1988.

[33] M. Griot, "CVI Melles Griot technical guide," vol. 2, no. 1, 2009.

[34] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "Quantum cryptography," *Reviews of modern physics*, vol. 74, no. 1, p. 145, 2002.

[35] G. P. Temporão, "Um polarímetro de baixo custo," Master's thesis, Pontifícia Universidade Católica do Rio de Janeiro, Departamento de Engenharia Elétrica, Curso de Pós-Graduação em Engenharia Elétrica, Rio de Janeiro, 2003.

[36] J.-M. Merolla, Y. Mazurenko, J.-P. Goedgebuer, and W. T. Rhodes, "Single-photon interference in sidebands of phase-modulated light for quantum cryptography," *Physical review letters*, vol. 82, no. 8, p. 1656, 1999.

[37] D. Stucki, N. Brunner, N. Gisin, V. Scarani, and H. Zbinden, "Fast and simple one-way quantum key distribution," *Applied Physics Letters*, vol. 87, no. 19, p. 194108, 2005.

[38] M. Almeida, S. Walborn, and P. S. Ribeiro, "Experimental investigation of quantum key distribution with position and momentum of photon pairs," *Physical Review A*, vol. 72, no. 2, p. 022313, 2005.

[39] C. Hong and L. Mandel, "Experimental realization of a localized one-photon state," *Physical Review Letters*, vol. 56, no. 1, p. 58, 1986.

[40] W.-Y. Hwang, "Quantum key distribution with high loss: toward global secure communication," *Physical Review Letters*, vol. 91, no. 5, p. 057901, 2003.

[41] A. Peres, *Quantum theory: concepts and methods*, ser. Fundamental Theories of Physics. Kluwer Academic Publishers, 2002, vol. 72.

[42] C. Gerry and P. Knight, *Introductory Quantum Optics*, 1st ed. New York, NY: Cambridge University Press, 2005.

[43] C. H. Bennett, "Quantum cryptography using any two nonorthogonal states," *Physical review letters*, vol. 68, no. 21, p. 3121, 1992.

[44] P. W. Shor and J. Preskill, "Simple proof of security of the bb84 quantum key distribution protocol," *Physical review letters*, vol. 85, no. 2, p. 441, 2000.

[45] M. Christandl, R. Renner, and A. Ekert, "A generic security proof for quantum key distribution," *arXiv preprint quant-ph/0402131*, 2004.

[46] B. Kraus, N. Gisin, and R. Renner, "Lower and upper bounds on the secret-key rate for quantum key distribution protocols using one-way classical communication," *Physical review letters*, vol. 95, no. 8, p. 080501, 2005.

[47] N. Jain, C. Wittmann, V. Makarov *et al.*, "Device calibration impacts security of quantum key distribution," *Physical Review Letters*, vol. 107, no. 11, p. 110501, 2011.

[48] S. Sajeed, P. Chaiwongkhot, V. Makarov *et al.*, "Security loophole in free-space quantum key distribution due to spatial-mode detector-efficiency mis-match," *Physical Review A*, vol. 91, no. 6, p. 062301, 2015.

[49] F. Xu, K. Wei, V. Makarov *et al.*, "Experimental quantum key distribution with source flaws," *Physical Review A*, vol. 92, no. 3, p. 032305, 2015.

[50] S. Sajeed, A. Huang, V. Makarov *et al.*, "Insecurity of detector-device-independent quantum key distribution," *Physical review letters*, vol. 117, no. 25, p. 250505, 2016.

[51] C. H. Bennett, G. Brassard, C. Crépeau, and U. M. Maurer, "Generalized privacy amplification," *IEEE Transactions on Information Theory*, vol. 41, no. 6, pp. 1915–1923, 1995.

[52] Tektronix. (2016) Arbitrary function generators-3000 series – datasheet. Acessado: 18–12–2019. [Online]. Available: http://www.testequipmentdepot.com/tektronix/pdf/afg3000c-series_datasheet.pdf

[53] ——. (2014) Arbitrary function generators-3000 series – manual. Acessado: 18–12–2019. [Online]. Available: https://www.tek.com/signal-generator/afg3000-function-generator-manual/afg3000-series-1

[54] ID Quantique SA. (2017) Id-210 infrared single-photon detector. Acessado: 20–12–2019. [Online]. Available: https://marketing.idquantique.com/acton/attachment/11868/f-0239/1/-/-/-/-/ID210_Brochure.pdf

[55] Opal Kelly. XEM3005 – Opal Kelly. Acessado: 20–12–2019. [Online]. Available: hhttps://opalkelly.com/products/xem3005/

[56] P. P. Chu, *Prototyping by VHDL Examples: Xilinx Spartan–3 Version*, 1st ed. Hoboken, New Jersey: Wiley Interscience, 2008.

[57] T. Sutili, "Estudo e caracterização experimental de modulador óptico em quadratura utilizando sinais em contra–fase," Master's thesis, Universidade Estadual de Campinas – Unicamp, Campinas – SP, 2014.

[58] G. Morelli and M. Morelli, "Obtenção e caracterização de pós de niobato de lítio," in *Anais do 44 Congresso Brasileiro de Cerâmica*, Mai–Jun 2000, pp. 11 101–11 112.

[59] EOSpace Inc. Low-loss and high-speed multi-stage polarization controller. Acessado: 20–12–2019. [Online]. Available: https://www.eospace.com/polarization-controller

[60] F. A. Rodrigues, "Transmissor óptico baseado no chaveamento de polarização da luz," Master's thesis, Pontifícia Universidade Católica do Rio de Janeiro – PUC-Rio, Rio de Janeiro – RJ, 2012.

[61] Boston Applied Technologies Inc. Acrobat polarization controller. Acessado: 20–12–2019. [Online]. Available: http://www.bostonati.com/products/PI%20sheet%20PC.pdf

[62] ——. Acrobat polarization controller. Acessado: 20–12–2019. [Online]. Available: http://www.optoceramics.com/products/pc1002.pdf

[63] General Photonics Corporation. (2013) Fiber–optic polarization tracker – Polastay POS–002. Acessado: 20–12–2019. [Online]. Available: https://www.generalphotonics.com/downloads/manuals/POS-002-Manual-V2-1-9-27-13.pdf

[64] T. Jennewein, C. Simon, G. Weihs, H. Weinfurter, and A. Zeilinger, "Quantum cryptography with entangled photons," *Physical Review Letters*, vol. 84, no. 20, p. 4729, 2000.

[65] D. Naik, C. Peterson, A. White, A. Berglund, and P. G. Kwiat, "Entangled state quantum cryptography: eavesdropping on the ekert protocol," *Physical Review Letters*, vol. 84, no. 20, p. 4733, 2000.

[66] D. Stucki, N. Gisin, O. Guinnard, G. Ribordy, and H. Zbinden, "Quantum key distribution over 67 km with a plug&play system," *New Journal of Physics*, vol. 4, no. 1, p. 41, 2002.

[67] L. Elterman, "Parameters for attenuation in the atmospheric windows for fifteen wavelengths," *Applied optics*, vol. 3, no. 6, pp. 745–749, 1964.

[68] R. J. Hughes, J. E. Nordholt, D. Derkacs, and C. G. Peterson, "Practical free-space quantum key distribution over 10 km in daylight and at night," *New Journal of Physics*, vol. 4, pp. 43–43, jul 2002.

[69] F. Ozek, "Potential application of laser diodes to free space optical communication between mobile on-sea terminals," *Physica Scripta*, vol. 63, no. 6, pp. 475–478, jun 2001.

[70] D. N. Harres, "Analog dividers for acquisition and tracking signal normalization," in *Free-Space Laser Communication Technologies II*, vol. 1218. International Society for Optics and Photonics, 1990, pp. 108–116.