Universidade Federal de Campina Grande
Centro de Engenharia Elétrica e Informática
Departamento de Engenharia Elétrica e Informática

Relatório de Estágio Supervisionado

QuantaC - Universidade Federal de Campina Grande

Henrique Jordão Figueiredo Alves

Campina Grande, PB
Dezembro de 2018

Henrique Jordão Figueiredo Alves

Relatório de Estágio Supervisionado

Relatório de estágio supervisionado apresentado à Coordenação do Curso de Graduação em Engenharia Elétrica da Universidade Federal de Campina Grande, Campus Campina Grande, como parte dos requisitos necessários para a obtenção do grau de Bacharel em Engenharia Elétrica.

Área de Concentração: Comunicação e Criptografia Quântica

Orientador: Leocarlos Bezerra da Silva Lima

Campina Grande, PB
Dezembro de 2018

Henrique Jordão Figueiredo Alves

Relatório de Estágio Supervisionado

Relatório de estágio supervisionado apresentado à Coordenação do Curso de Graduação em Engenharia Elétrica da Universidade Federal de Campina Grande, Campus Campina Grande, como parte dos requisitos necessários para a obtenção do grau de Bacharel em Engenharia Elétrica.

Aprovado em ___/___ /___

Professor Avaliador
Universidade Federal de Campina Grande
Avaliador

Leocarlos Bezerra da Silva Lima
Universidade Federal de Campina Grande
Orientador

Agradecimentos

Gostaria de agradecer primeiramente a Deus, que apesar de todas as dificuldades sempre esteve ao meu lado e garantiu que tudo pudesse dar certo no final.

Aos meus pais, Alexandro Alves e Maria Solange, por sempre terem feito de tudo para me fornecer a melhor formação possível e sempre demonstrarem apoio quanto às minhas decisões.

Ao meu irmão Hugo, pelas alegrias que este me proporciona desde o seu nascimento.

Aos meus colegas de curso, pelo companheirismo e pela ajuda mútua na qual compartilhamos ao longo do curso. Cito alguns, Jefferson Albuquerque, Thiago Ribeiro Félix, Marcelo Meneses, Michael Douglas, Leonardo Dantas, Matheus Andrade, Jesney Pires, dentre outros.

Ao meu orientador, profº Leocarlos Bezerra, por ter me oferecido a oportunidade desse estágio.

Ao aluno de mestrado, Micael Andrade Souza, por ter me acompanhado durante a montagem dos experimentos e por tentar me passar a maior quantidade de informações possíveis para o entendimento do trabalho.

”Eu não tenho tempo para uma esposa e um avião.”
Wilbur Wright

Resumo

Este trabalho apresenta as atividades realizadas durante a vigência da disciplina de Estágio Supervisionado, feita pelo aluno de graduação em Engenharia Elétrica pela Universidade Federal de Campina grande (UFCG), Henrique Jordão Figueiredo Alves. O estágio foi realizado nas dependências do Laboratório QuantaC (UFCG), onde foram feitos experimentos e montagens relacionados aos princípios da criptografia quântica. Esses experimentos incluem: fusão de fibras ópticas, montagem do Interferômetro de Mach-Zehnder, dentre outros.

Palavras chave: Criptografia Quântica, Interferômetro de Mach-Zehnder, fibra óptica.

Abstract

This work presents the activities carried out during the validity of the Supervised Internship, made by the undergraduate student in Electrical Engineering at the Federal University of Campina Grande (UFCG), Henrique Jordão Figueiredo Alves. The stage was carried out in the premises of the QuantaC Laboratory (UFCG), where experiments and assemblages related to the principles of quantum cryptography were made. These experiments include: fusion of optical fibers, assembly of the Mach-Zehnder Interferometer, among others.

Keywords: Quantum Cryptography, Mach-Zehnder Interferometer, optical fiber.

Lista de Figuras

Lista de Abreviaturas e Siglas

A	Alice
B	Bob
BS	Beam Splitter
CP	Controlador de Polarização
D	Base Diagonal
dBm	decibel miliwatt
F	Espelho de Faraday
I	Inteferômetro
IM	Modulador de Intensidade
L	Laser
PM	Modulador de Fase
R	Base Retilínea

Sumário

1 Introdução

Este relatório descreve as atividades referentes à disciplina de Estágio Supervisionado, com carga horária de 180h. As tarefas foram realizadas no Laboratório de Comunicações Quânticas (QuantaC) - UFCG, durante o período de 27 de agosto de 2018 à 16 de Novembro de 2018, sob a orientação do professor Leocarlos Bezerra da Silva Lima e a supervisão do técnico Ronaldo Araújo Alves.

O estágio teve como principal objetivo a contribuição na implementação do protocolo BB84 para distribuição quântica de chaves. Outras tarefas desempenhadas foram de familiarizar-se com os equipamentos do QuantaC, tais como: modulador ótico de fase, beam splitter, contador de fótons, atenuador, máquina de fusão de fibras óticas, OTDR, etc, e por fim, a montagem e experimentação de um interferômetro de Mach-Zehnder.

1.1 Local de Estágio

O estágio supervisionado foi realizado no Laboratório de Comunicações Quânticas (QuantaC), localizado no Bloco CJ, na Universidade Federal de Campina Grande.

1.2 Objetivo

Realizar e implementar o protocolo de distribuição de chaves quânticas BB84 assim como a montagem e a realização de experimentos com o interferômetro de Mach-Zehnder.

2 Fundamentação Teórica

Nessa seção será detalhada a fundamentação teórica com a apresentação dos conceitos necessários para o desenvolvimento do trabalho realizado.

2.1 A Criptografia e a Distribuição de Chaves

Os sistemas criptográficos servem para cifrar uma escrita de forma em que esta se torna ininteligível para aqueles que não possuem a chave que dá acesso à informação contida na mensagem. Estes podem ser divididos em dois tipos de algoritmos, os de criptografia simétrica e assimétrica.

Simétrica: são algoritmos para criptografia que usam a mesma chave criptográfica para cifragem de texto puro e decifragem de texto cifrado.

Assimétrica: também conhecido como criptografia de chave pública, é qualquer sistema criptográfico que usa pares de chaves: chaves públicas, que podem ser amplamente disseminadas, e chaves privadas que são conhecidas apenas pelo proprietário, seja ele o remetente ou o destinatário.

Dentro desse contexto, temos que, apesar da consolidação de certos algoritmos criptográficos de chave pública (Ex: o RSA) nos processos de transmissão de mensagens, é bem provável que, ao passar dos anos, com o avanço da tecnologia e a evolução dos computadores quânticos, esses sistemas mais comuns que conhecemos hoje, sejam facilmente quebrados num futuro próximo. Daí, surge a necessidade de se utilizar um novo modelo de segurança na comunicação. É o caso da chamada **criptografia quântica**.

2.2 Criptografia Quântica

A criptografia quântica se destaca frente aos outros métodos criptográficos por não necessitar de comunicações secretas prévias, permitir a detecção de intrusos e ser segura mesmo que o intruso possua um poder computacional ilimitado, pois esta se baseia em leis da física, enquanto as demais garantem apenas a segurança com base na limitação computacional na fatoração de números primos com muitos dígitos, os logaritmos discretos, entre outros.

2.2.1 O Qubit

Ao passo que o bit é a unidade fundamental dos sistemas clássicos de informação, assumindo um valor binário 0 ou 1, o campo da informação quântica faz uso de uma unidade distinta: o qubit, ou bit quântico. Um qubit pode ser representado como um vetor unidimensional, em um espaço vetorial complexo de duas dimensões. Para sua representação, se utiliza a notação bra-ket de Dirac para os estados quânticos do qubit, conforme mostrada na Equação 1, para um dado qubit:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \tag{1}$$

Os estados $|0\rangle$ e $|1\rangle$ formam uma base para o espaço vetorial bidimensional supracitado, enquanto α e β são números complexos obedientes à Equação 2.

$$|\alpha|^2 + |\beta|^2 = 1 \tag{2}$$

Isso significa que o estado de um qubit é uma combinação linear dos estados $|0\rangle$ e $|1\rangle$, ponderados pelos fatores complexos alfa e beta, a serem escrutinados com mais detalhe em seção posterior. Múltiplos qubits podem ter seus estados quânticos descritos por produtos tensoriais de seus estados correspondentes, de tal sorte que n qubits habitam um espaço vetorial n-dimensional.

2.2.2 Fótons, Estados Quânticos e Bases Conjugadas

Fótons são as partículas básicas elementares da luz e que têm como característica a dualidade onda-partícula. No contexto da criptografia quântica, podem ser polarizados, tais quais on-

das magnéticas senoidais, de modo a adquirir comportamentos desejados de acordo com as circunstâncias em que se encontram e conforme as propriedades previstas pela física quântica.

As bases conjugadas e não-ortonormais entre si são formadas por vetores ortonormais, que definirão, com a polarização posterior, a orientação dos qubits avaliados.

No protocolo BB84, discutido mais adiante, são consideradas a Base Retilínea (R), composta de polarizações em ângulos de 0º (estado $|0\rangle$) e 90º (estado $|1\rangle$), e a Base Diagonal (D), dispondo de polarizações em 45º (estado $|+\rangle$) e 135º (estado $|-\rangle$). Vale salientar que os estados da Base Diagonal podem ser decompostos em função dos estados da Base Retilínea, seguindo as Equações 3 e 4:

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

$$|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \tag{4}$$

Os estados quânticos resultantes das duas bases são, portanto, $|0\rangle$, $|1\rangle$ para a Base R, e $|+\rangle$, $|-\rangle$ para a Base D, e estão exibidos graficamente nas Figuras 2.1 e 2.2.

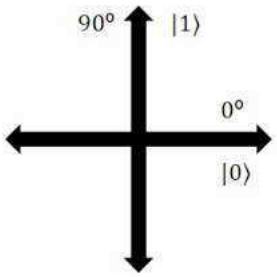

Figura 2.1: Base Conjugada Retilínea

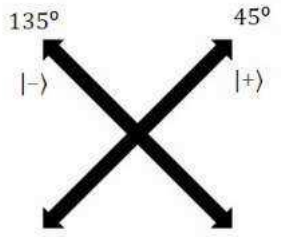

Figura 2.2: Base Conjugada Diagonal

A medição de um dado qubit $|\psi\rangle$, conforme a notação estabelecida, será realizada em uma base arbitrada. Na física quântica, a medição de um qubit $|\psi\rangle$ utilizando a base genérica ($|c\rangle$,$|g\rangle$)

resultará nos estados definidos pela base com probabilidades iguais aos termos complexos que as multiplicam. Isto é, da Equação 1, definindo o qubit na base $|0\rangle$, $|1\rangle$ e medindo-o na mesma, obtêm-se o estado $|0\rangle$ com probabilidade $|\alpha|^2$ e o estado $|1\rangle$ com probabilidade $|\beta|^2 = 1$. Naturalmente, a soma dessas probabilidades é unitária, satisfazendo a Equação 2.

2.3 O protocolo BB84

O principal protocolo da criptografia quântica atualmente foi criado em 1984 por Charles Bennett e Gilles Brassard. Daí o nome BB84, em alusão às primeiras letras de seus nomes e ao ano em que foi implementado.

Consideremos dois indivíduos convencionalmente intitulados como, Alice e Bob, que querem se comunicar trocando informações ou mensagens, e de repente um intruso, chamado Eve, intercepta a comunicação entre ambos.

Quando o remetente Alice (A) quer enviar a chave gerada por partículas de luz de fótons polarizados para o destinatário Bob (B). Ela transfere cada bit de fóton específico de forma arbitrária, selecionando as duas bases arbitrárias de fótons polarizados, retilínea ou diagonal. O destinatário B pode escolher aleatoriamente o polarizador retilíneo ou diagonal para calcular os fótons que recebeu e informa o resultado ao remetente A, através de qualquer canal inseguro. Depois de comparar os bits recebidos do destinatário, finalmente eles descartam os bits incorretos e usam o correto como chave [1].

2.4 Interferômetro de Mach-Zehnder

O **Interferômetro de Mach-Zehnder** é um experimento de óptica que foi realizado pela primeira vez no final do século XIX pelos físicos Ludwig Mach (1868-1949) e Ludwig Zehnder (1854-1949). O arranjo permite realizar experimentos de interferência, difração e polarização com um feixe de luz de baixa intensidade, em que a interação da luz com o interferômetro ocorre de fóton em fóton. Na Figura 2.3 abaixo, é possível visualizar melhor o arranjo experimental realizado por Mach e Zehnder.

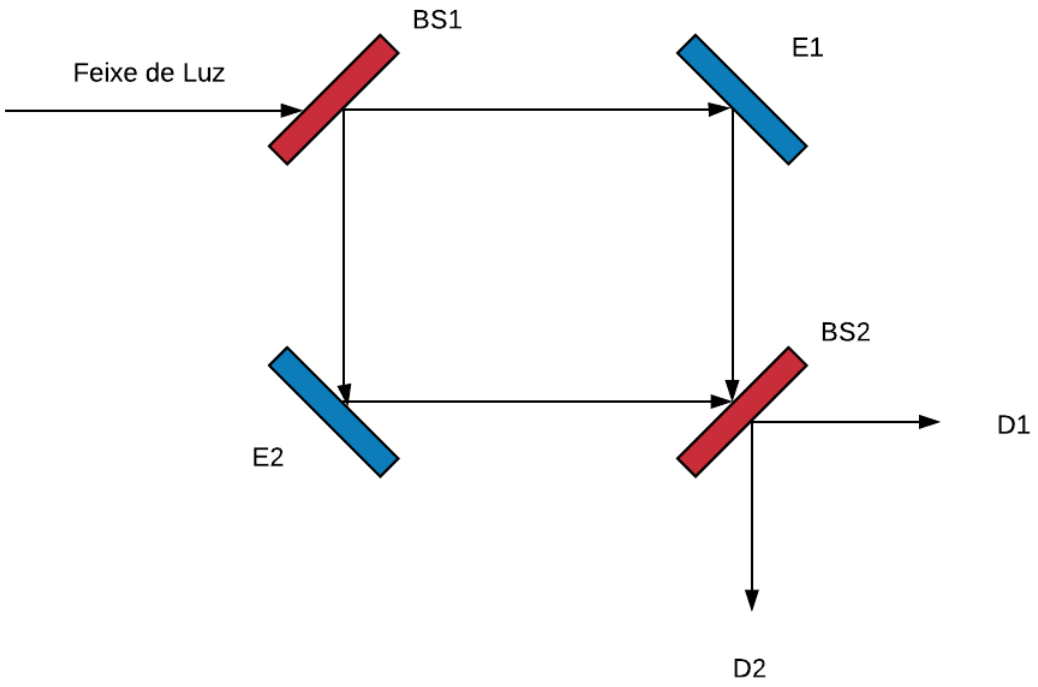

Figura 2.3: Interferômetro de Mach-Zehnder

Um fóton incide sobre um *beam-splitter* (divisor de feixe), que nada mais é do que um espelho semi-prateado que reflete 50% do feixe incidente e transmite os outros 50%. As superfícies refletoras dos divisores de feixe seriam orientadas de modo que os feixes de teste e de referência passem através de uma quantidade igual de vidro. Nessa orientação, os feixes de teste e referência experimentam, cada um, dois reflexos na superfície frontal, resultando no mesmo número de inversões de fase. O resultado é que a luz percorrendo um caminho ótico igual, nos feixes de teste e referência, produza uma franja de luz branca de interferência construtiva [2]. Os espelhos E1 e E2 são refletores perfeitos que geram uma nova superposição de estados quânticos para o divisor BS2, que por sua vez contém uma fase que depende da diferença dos caminhos ópticos. D1 e D2 representam os detectores de fótons resultantes da interação.

Durante o estágio, o interferômetro foi montado utilizando acopladores de fibras ópticas como *beam splitters*.

3 Equipamentos Utilizados

Nesta seção serão detalhados os equipamentos que foram utilizados para a implementação do protocolo BB84 e montagem do interferômetro. Todos os equipamentos utilizados na montagem são da marca Thorlabs® [1].

3.1 Fibra Óptica

Eis o material base da montagem, a **fibra óptica**. A fibra óptica é um filamento de vidro bastante fino (similar ao fio de cabelo humano) que possui uma camada de revestimento e de refração sobre a camada do seu núcleo. É através da refração de luz elevadíssima do núcleo da fibra que permite esta a transmitir luz entre uma extremidade e a outra.

Figura 3.1: Fibra Óptica

Nas seguintes subseções, serão detalhados os equipamentos utilizados a base de fibras ópticas.

3.1.1 Circulador Óptico

O circulador óptico é um componente à fibra que possui três portas ópticas. Um sinal óptico injetado na porta 1 sai na porta 2 e um sinal óptico entrando pela porta 2 sai na porta 3 (ver Figura 3.3). Os circuladores são usados em transmissão bidirecional em fibra e serve para injetar ou extrair sinais sendo transmitidos. Possuem uma baixa perda de inserção e alta isolação entre as portas. Estes componentes operam em comprimentos de onda bem definidos e com uma banda da ordem de 20 a 30 nm.

[1] www.thorlabs.com

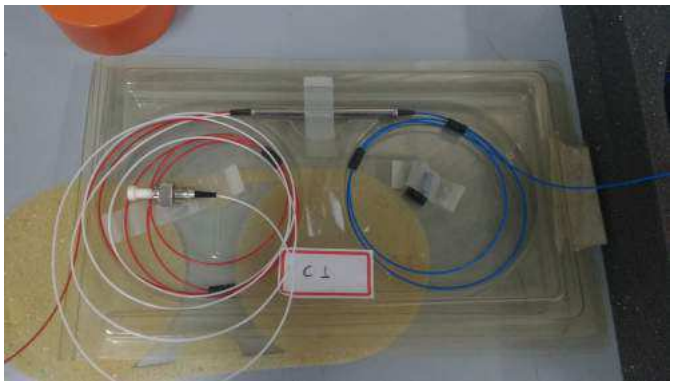

Figura 3.2: Circulador Óptico

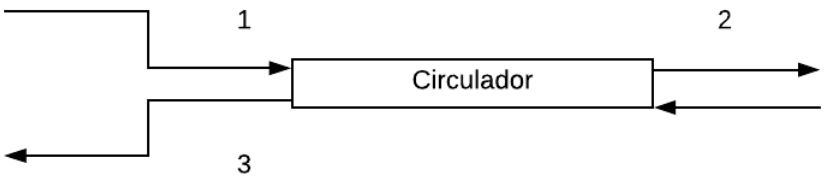

Figura 3.3: Esquema de funcionamento do Circulador Óptico

3.1.2 Modulador de Fase e Intensidade

Um modulador óptico de intensidade é um dispositivo que é usado para modular um feixe de luz transmitido através das fibras ópticas. Dependendo da característica da manipulação do feixe, os moduladores podem ser de fase, intensidade, etc. Essa modulação ocorre por meio da regulação de corrente elétrica que é enviada por uma fonte de luz, no caso da montagem, um diodo laser.

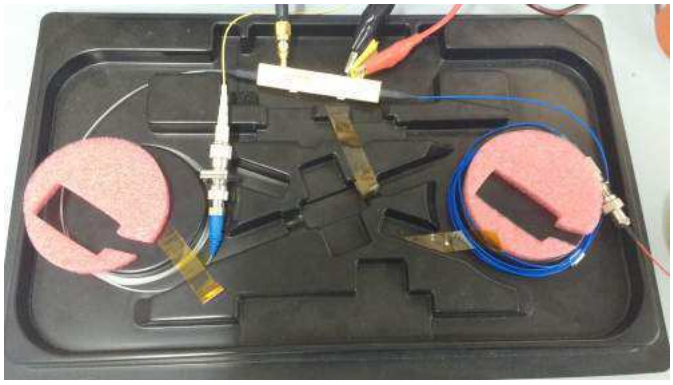

Figura 3.4: Modulador de Intensidade

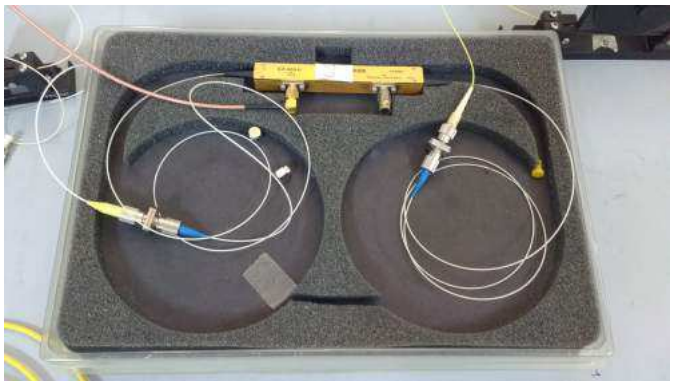

Figura 3.5: Modulador de Fase

3.1.3 Controlador de Polarização

O controlador de polarização é um dispositivo óptico que permite modificar o estado de polarização da luz.

Os controladores de polarização são operados normalmente por ajuste manual ou por sinais elétricos de um gerador. Ele pode ter uma tarefa de transformar uma polarização fixa e conhecida em uma polarização arbitrária.

Os controladores de polarização podem ser implementados com óptica de espaço livre, por meio de fibras ópticas. Nesse caso, a luz sai da fibra, passa pelas três placas de onda, que podem ser giradas livremente para permitir o ajuste de polarização e, em seguida, entra de volta na fibra.

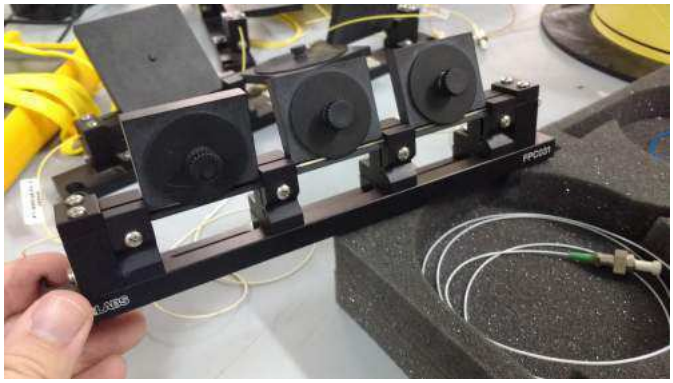

Figura 3.6: Controlador de Polarização

3.1.4 Beam Splitter

O *Beam Splitter*, ou divisor de feixe, é um dispositivo designado para dividir o feixe de luz em dois.

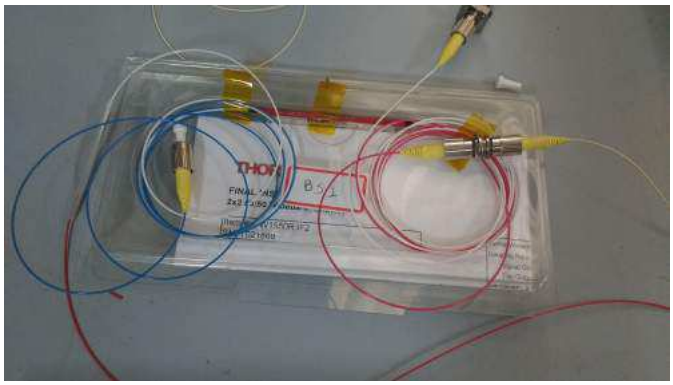

Figura 3.7: Beam Splitter

3.1.5 Espelho de Faraday

Os Espelhos Faraday com uma *pigtail* de fibra óptica são dispositivos projetados para retornar a luz com uma polarização ortogonal de 90º em relação ao estado de polarização de entrada. Esses dispositivos fornecem uma alta relação sinal-ruído, o que os tornam ideais para uso do interferômetro de fibra óptica.

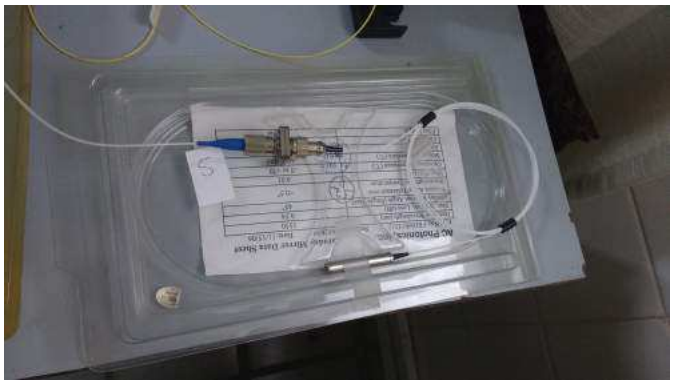

Figura 3.8: Espelho de Faraday

3.2 Máquina de Fusão

A máquina de fusão é um pequeno aparelho destinado à realização de fusões de fibras ópticas. Boa parte dos equipamentos descritos na seção anterior foram montados com o auxílio da máquina de fusão, bem como acidentes envolvendo a quebra de fibras ópticas.

Figura 3.9: Máquina de Fusão

3.3 Medidor de Potência

O medidor de potência é um dispositivo para medir a potência absoluta na escala logarítmica em uma ponta de fibra óptica. Os seus valores são lidos em dBm (decibel miliwatt).

Figura 3.10: Medidor de Potência

4 Montagem

Nesta seção serão detalhados os trabalhos realizados no laborátorio QuantaC durante a vigência do estágio, visando cumprir ao máximo as metas e objetivos pré-definidos.

4.1 Montagem Inicial de Implementação do BB84

Como ponto de partida, foi realizada a montagem dos equipamentos presentes no laboratório a fim de realizar a implementação do protocolo BB84. Na montagem, foram utilizados os equipamentos já previamente mostrados na seção anterior. O esquemático para a montagem pode ser conferido na Figura 4.1 logo abaixo.

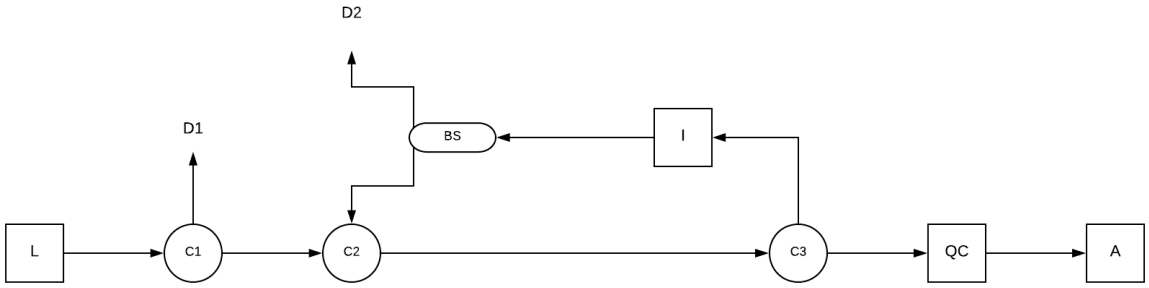

Figura 4.1: Esquemático da Montagem do Experimento

Onde:

- L representa o controlador de temperatura e o laser do sistema;
- C1, C2 e C3 são os circuladores ópticos;
- BS é o *beam splitter*;
- I representa o interferômetro;
- QC é o canal quântico;
- A é o receptor da informação do sistema (no nosso caso Alice);
- D1 e D2 são os detectores de fótons.

Durante a primeira semana, foi realizado um estudo mais centrado no protocolo BB84 e uma maior familiarização com os equipamentos necessários para a realização do experimento.

4.1.1 Fusão de Fibras Ópticas

No início do estágio, boa parte do experimento já se encontrava montado, porém certos acidentes podem ocorrer com frequência caso não haja um certo cuidado no manuseio das fibras ópticas, pois afinal elas possuem uma camada interna muito frágil. Assim como foi feito para montagem de alguns equipamentos, também há a necessidade de realizar uma **fusão de fibras ópticas** em casos de quebras das mesmas. Para isso foi-se necessário o uso da máquina de fusão (ver Figura 3.9).

Como já constatado anteriormente, a fibra óptica é frágil e este fato torna o trabalho de fusão entre duas fibras algo bastante delicado. Portanto, foi preciso ter um certo cuidado na hora de realizar o processo de fusão entre elas. Para esta atividade, seguiu-se o seguinte passo a passo:

1. Desencapamento das duas fibras até o revestimento de seu núcleo.
2. Limpeza das fibras com álcool.
3. Realizar a clivagem das fibras para terem o comprimento desejado.
4. Realizar o alinhamento automático das fibras com o auxílio da máquina de fusão.
5. Realizar a fusão.

Caso a fusão não apresente uma perda (em dB) relativamente baixa o processo acima precisará ser repetido.

Figura 4.2: Fusão sendo realizada pela Máquina de Fusão

Após a fusão ser bem-sucedida é preciso também injetar um bastolete que proteja a área onde foi realizada a fusão. Para isso, colocou-se o tubo de proteção na região onde as fibras se fundiram e depois a ajustamos ao dispositivo de aquecimento da máquina de fusão. Após certo tempo, o aquecimento estará completo e a nova fibra pôde vir a ser utilizada.

4.1.2 Princípios de Funcionamento Gerais da Montagem

Após realizar todas as fusões necessárias, bem como os ajustes finais dos equipamentos, partimos então agora para a execução dos testes e demais experimentos com o aparelho.

Inicialmente liga-se o controlador de temperatura, em seu ajuste padrão de 10kΩ, e em seguida o laser, que é o responsável pela transmissão de luz de Bob para Alice. Para não causar erros de leitura de potência futuras, ajustou-se o laser para potência zero (0dB). A luz transmitida será modulada pelo modulador de intensidade.

Antes da luz passar pelo modulador, há um controlador de polarização para controlar a potência de saída. Os ajustes feitos pelo controlador são realizados, tal que, a amplitude em sua saída seja a maior possível. O mesmo procedimento vale para todo modulador presente na montagem, seja ele de intensidade ou de fase.

Após a luz ser modulada, a mesma irá passar pelos circuladores C1, C2 e C3 presentes na Figura 4.1 até o canal quântico, onde serão transmitidos as informações quânticas da luz para Alice. Na montagem, o canal quântico é uma bobina de fibra óptica.

Após isso, a luz passa por um *beam-splitter* que a divide em dois feixes: um para um detector de sincronização (um chip FPGA), e o outro para um trecho de *delay* (atraso) de informação. Esse atraso ocorre para dar tempo ao detector de sincronização realizar a programação. Assim como o Canal Quântico, o trecho de atraso também é representando por uma bobina de fibra óptica.

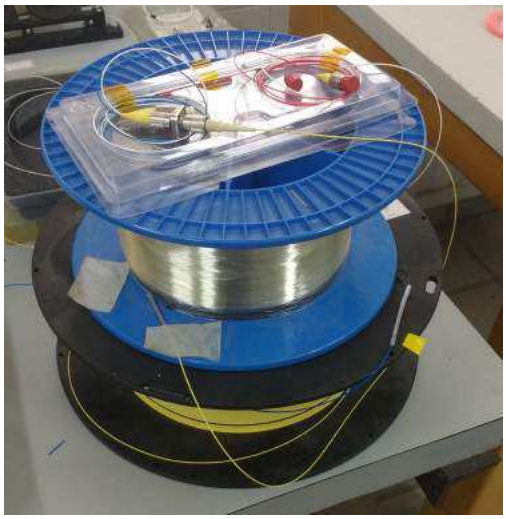

Figura 4.3: Canal Quântico (bobina de cima) e trecho de atraso (bobina de baixo)

Após passar pelo *delay* o pulso de luz é atenuado e passa pelo modulador de fase, que determina a escrita da informação no fóton que chega para Alice.

Alice portanto irá escolher uma de quatro fases possíveis (0^o, 45^o, 90^o ou 135^o) aleatoriamente, através de uma sequência de bits e outra de bases conjugadas. Essa sequência de bits e bases feitas

por Alice é que irá determinar a fase por ela escolhida. Esse procedimento é feito pelo detector de sincronização. Assim, o fóton chega ao espelho de Faraday, que irá transportá-lo de volta a Bob fazendo o caminho reverso, porém desta vez passando pelo interferômetro.

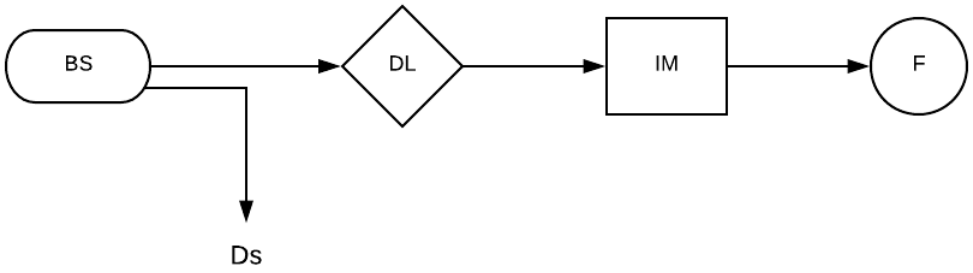

Figura 4.4: Esquemático do processo de escrita da informação para Alice

4.2 Princípios de Funcionamento e Montagem do Interferômetro de Mach-Zehnder

Nesta seção serão abordados os princípios de funcionamento do interferômetro dentro do protocolo BB84, bem como os procedimentos feitos para validar a legitimidade do interferômetro.

4.2.1 Funcionamento Geral do Interferômetro

Após Alice realizar a escolha da fase, o fóton retorna pelo caminho reverso, porém ao chegar ao circulador C3 ele é "*bybassado*"e acaba por cortar caminho pelo interferômetro. O desenho esquemático do interferômetro se encontra na Figura 4.5.

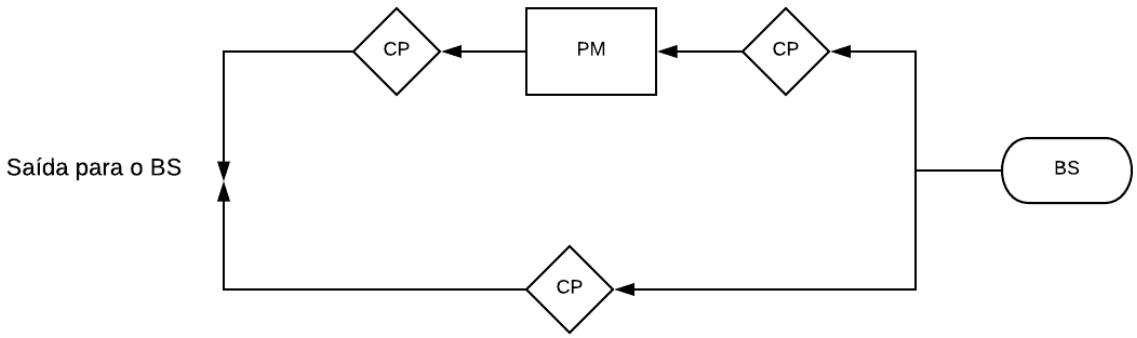

Figura 4.5: Esquemático da montagem do Interferômetro

Ao chegar no *beam-splitter*, o fóton entra em superposição, gerando assim um estado quântico. Uma parte da superposição é modulada pelo modulador de fase (PM), porém desta vez será uma medição projetiva. Essa projeção será ortogonal, onde um outro FPGA gera outra sequência de bases aleatória para cada estado quântico de Alice.

Essa sequência de bases é comparada com a fase determinada por Alice. Quanto mais fótons o sistema envia, a probabilidade de acerto na tentativa do intruso em decriptar a mensagem é limitada em até 50%, pois os FPGAs irão gerar no mínimo de duas bases na sequência. Quanto mais bases forem geradas, tanto para Alice quanto para Bob, mais seguro é o sistema.

4.2.2 Montagem do Interferômetro

Após a montagem da primeira parte do aparelho, finalizando a conexão entre Bob e Alice, o interferômetro poderá ser testado separadamente. Para que o interferômetro funcione sem problemas, ou seja, que cause uma interferência capaz de realizar inversão de fase do estado quântico, é preciso que cada um dos seus braços possua a mesma potência.

Para isso, primeiramente desconectou-se a conexão do interferômetro com Alice, assim como o braço inferior do *beam-splitter* e passamos a medir a potência de saída do braço superior quando este recebe um feixe de luz vindo do laser. O modulador de intensidade do laser e o modulador de fase do interfeômetro também foram desligados temporariamente. Os controladores de polarização foram ajustados para que obtivéssemos a maior potência possível. Através do medidor de potência, anotamos o valor de -9.3 dBm.

Agora que já medimos a potência máxima do braço superior, realizamos o mesmo procedimento para o braço inferior, desconectando o braço superior da ligação com o laser. Com o auxílio dos controladores de polarização, foi possível manter o valor de -9.3 dBm igual ao outro braço.

Agora com ambos os braços ajustados para apresentarem a mesma potência, um teste de medição é realizado com ambos os braços ligados ao laser. Segundo a escala logarítmica, o dobro de uma potência em dBm é o mesmo que somar em 3 o seu valor. Logo, a potência do interferômetro com ambos os braços recebendo feixe de luz, com os moduladores desligados, foi de aproximadamente -6 dBm, confirmando-se com a teoria. Com o modulador de intensidade regulando a amplitude do feixe de luz, ambos os braços terão o valor de -16.3 dBm separadamente e -13 dBm em conjunto.

Até o momento, tudo ocorre perfeitamente bem para o funcionamento adequado do interferômetro, porém resta saber se o sinal de saída do aparelho pode apresentar uma inversão de fase quando se aplica uma tensão em seu modulador de fase. Portanto, é necessário saber qual a tensão exigida pelo modulador para inverter a fase do sinal e gerar interferência no sistema de troca de mensagens.

Através de um gerador de sinais, diversos valores de tensão foram aplicados na entrada do modulador de fase, porém nenhum resultado satisfatório era obtido pelo osciloscópio, com o sinal apresentando pouquíssima ou quase nenhuma interferência.

Por outro lado, ao analisar alguns manuais dos componentes em questão, percebeu-se que o modulador de intensidade possui características similiares a de um interferômetro. Logo, decidiu-se substituir os componentes que faziam parte da montagem do aparelho por um dos moduladores de intensidade reservas. Ao aplicar uma tensão em sua entrada, descobrimos que o comportamento do componente remete a possibilidade do mesmo funcionar da mesma forma que um interferômetro, pois ao atingir a marca de 2.5 V, o mesmo têm a fase de seu sinal de saída invertida, de acordo com o esperado.

Figura 4.6: Montagem do experimento completo

5 Conclusão

Durante o estágio foi possível realizar boa parte das atividades propostas e realizar testes com os equipamentos para as montagens.

Infelizmente, não foi possível determinar com precisão se a montagem original do interferômetro pode vir a ser utilizada para trabalhos futuros, porém sugere-se que se realize mais alguns testes com o modulador de intensidade, como interferômetro, para se ter a certeza de que o componente pode, de fato, ser uma solução ao problema em questão.

Para trabalhos futuros, sugere-se empregar os dispositivos FPGA para a realização de testes, para com as sequências de bases e bits por eles geradas, além de realizar um estudo e testes com os detectores de fóton para finalizar a implementação do protocolo BB84.

Referências

[1] MOIZUDDIN, Mohammed; WINSTON, Joy; QAYYUM, Mohammed. A comprehensive survey: Quantum cryptography. In: *Anti-Cyber Crimes (ICACC) 2nd International Conference on.* IEEE, 2017.

[2] ZETIE, K. P.; ADAMS, S. F.; TOCKNELL, R. M. How does a Mach-Zehnder interferometer work?. *Physics Education*, v. 35, n. 1, p. 46, 2000.

[3] J. TOWNSEND: A Modern Approach to Quantum Mechanics, 1st edition. *University Science Books: Clare-mont* 2000.