UNIVERSIDADE FEDERAL DO CEARÁ

CENTRO DE TECNOLOGIA

DEPARTAMENTO DE ENGENHARIA DE TELEINFORMÁTICA

PROGRAMA DE PÓS-GRADUAÇÃO EM ENGENHARIA DE TELEINFORMÁTICA

ANTÔNIO GEOVAN DE ARAÚJO HOLANDA GUERRA

COMUNICAÇÃO QUÂNTICA SEGURA DIRETA E POLARIZAÇÃO QUÂNTICA USANDO ESTADOS CONTÍNUOS DA LUZ

FORTALEZA

2017

ANTÔNIO GEOVAN DE ARAÚJO HOLANDA GUERRA

COMUNICAÇÃO QUÂNTICA SEGURA DIRETA E POLARIZAÇÃO QUÂNTICA USANDO ESTADOS CONTÍNUOS DA LUZ

Tese apresentada ao Programa de Pós-Graduação em Engenharia de Teleinformática da Universidade Federal do Ceará, como requisito parcial à obtenção do título de Doutor em Engenharia de Teleinformática. Área de concentração: Eletromagnetismo Aplicado.

Orientador: Prof. Dr. Rubens Viana Ramos.

FORTALEZA

2017

Dados Internacionais de Catalogação na Publicação
Universidade Federal do Ceará
Biblioteca Universitária
Gerada automaticamente pelo módulo Catalog, mediante os dados fornecidos pelo(a) autor(a)

G963c Guerra, Antônio Geovan de Araújo Holanda.
Comunicação quântica segura direta e polarização quântica usando estados contínuos da luz / Antônio Geovan de Araújo Holanda Guerra. – 2017.
89 f.: il. color.

Tese (doutorado) – Universidade Federal do Ceará, Centro de Tecnologia, Programa de Pós-Graduação em Engenharia de Teleinformática, Fortaleza, 2017.
Orientação: Prof. Dr. Rubens Viana Ramos.

1. Comunicação quântica segura direta. 2. Distribuição quântica de chave. 3. Detecção homódina. 4. Polarização quântica. I. Título.

CDD 621.38

ANTÔNIO GEOVAN DE ARAÚJO HOLANDA GUERRA

COMUNICAÇÃO QUÂNTICA SEGURA DIRETA E POLARIZAÇÃO QUÂNTICA USANDO ESTADOS CONTÍNUOS DA LUZ

Tese apresentada ao Programa de Pós-Graduação em Engenharia de Teleinformática da Universidade Federal do Ceará, como requisito parcial à obtenção do título de Doutor em Engenharia de Teleinformática. Área de concentração: Eletromagnetismo Aplicado.

Aprovada em: 29 / 06 / 2017.

BANCA EXAMINADORA

_____

Prof. Dr. Rubens Viana Ramos (Orientador)
Universidade Federal do Ceará (UFC)

_____

Prof. Dr. João Batista Rosa Silva
Universidade Federal do Ceará (UFC)

_____

Profa. Dra. Hilma Helena Macedo de Vasconcelos
Universidade Federal do Ceará (UFC)

_____

Prof. Dr. Antonio Vidiella Barranco
Universidade Estadual de Campinas (UNICAMP)

_____

Prof. Dr. Marcos Cesar de Oliveira
Universidade Estadual de Campinas (UNICAMP)

Aos meus pais: Guazil (Gê) e Fátima.

Aos meus irmãos: George e Jean.

À minha noiva Heleninha e sua família.

Aos meus sobrinhos (as): Ana Lívia, Lucas, Heitor, Fátima, Théo e os demais que virão.

A toda minha família: tios (as); avós; primos (as) e em especial: Vanilda, Assunção, Maria Vilany, Socorrinha, Virgínia, Géssica, e João Miguel.
Aos meus padrinhos: Marta e Edvardo; Vanilda.

A todos os meus amigos e professores com quem convivi durante esses 11 anos de vida acadêmica.

Em especial: Edilson Siridó; Renato e Antônio (tios).

Dedico!

AGRADECIMENTOS

A Deus.

A toda minha família pelo incentivo nessa longa caminhada.

Ao meu estimado amigo e orientador Rubens Viana pela sua dedicação e paciência e por seus conhecimentos que me foram passados, que foi de muita importância para elaboração desta Tese.

Aos meus amigos e professores do GIQ: João e Hilma pelos ensinamentos e contribuições para minha formação; Paulo Régis, Paulo Vinícius, Fernando, Franklin, Glaucionor, Ranara, Fátima, Emanoela, George, Claudomir, Samy, Antônio, Paulo Brown, Leonardo, Tahim, Alax, Daniel, Natália, Aline, Gisele e Jeová.

Ao CNPq, pelo financiamento do projeto que resultou nesta tese, e à CAPES, pelo custeio dos meus estudos de Pós-graduação.

“A preguiça é a pobreza do mundo.”

(Edilson Siridó)

“Eu não creio que exista algo mais emocionante para o coração humano do que a emoção sentida pelo inventor quando ele vê alguma criação da mente se tornando algo de sucesso. Essas emoções fazem o homem esquecer comida, sono, amigos, amor, tudo.”

(Nikola Tesla)

RESUMO

A presente tese pode ser dividia em três partes: I) Protocolos de comunicação quântica Segura Direta (QSDC). II) Detecção homódina de fótons. III) Polarização quântica da luz. No que diz respeito aos protocolos de QSDC, três novos esquemas ópticos foram propostos. Estes protocolos utilizam a distribuição espectral das fontes luminosas e o uso de moduladores de fase dependentes da frequência para aumentar a segurança. No que concerne à detecção de fótons, foi realizado um experimento de detecção homódina de fótons. Nesse experimento mostrou-se que o sinal analógico transportado por um estado coerente fortemente atenuado pode ser recuperado por um receptor óptico baseado em um fotodiodo PIN. Por fim, na parte de polarização quântica da luz foi proposta uma nova medida de grau de polarização baseada na entropia de Shannon, bem como foi feito o cálculo do grau de polarização de estados contínuos de um fóton e coerentes. Foram também realizados dois experimentos para estimar o grau de polarização através da medição da visibilidade de polarização. Duas situações foram consideradas: o uso de um canal despolarizante e o laser semicondutor trabalhando em diferentes regimes de operação.

Palavras-chave: Comunicação quântica segura direta. Distribuição quântica de chave. Detecção homódina. Polarização quântica.

ABSTRACT

This thesis can be divided in three parts: I) Quantum secure direct communication protocols (QSDC). II) Homodyne single-photon detection. III) Quantum light polarization. Regarding the QSDC protocols, three new optical schemes were proposed. These new protocols use the spectral distribution of the light source and the frequency dependence of phase modulators in order to increase the security. In what concerns the single-photon detection, a homodyne single-photon detection experiment was realized. This experiment shows that an analog signal carried by a strongly attenuated coherent state can be recovered by an optical detector based on a PIN photodiode. At last, in the quantum polarization part, a new degree of polarisation measure based on the von Neumann entropy was proposed, as well the calculation of the quantum degree of polarization of continuum single-photon and coherent state was realized. Moreover, two experiments aiming to estimate the degree of polarisation by measuring the polarisation visibility were realized. Two situations were considered, the usage of a depolarizing channel and the semiconductor laser source working in different regimes of operation.

Keyword: Quantum secure direct communication. Quantum key distribution. Homodyne detection. Quantum polarization.

LISTA DE FIGURAS

LISTA DE TABELAS

SUMÁRIO

1 INTRODUÇÃO

Os trabalhos pioneiros de Bennett e Brassard (1984) com o protocolo de distribuição quântica de chaves (*quantum key distribution* - QKD) BB84 e Ekert (1991) com o protocolo E91, mostraram como explorar recursos quânticos para fins criptográficos. Especificamente, o uso de estados quânticos não ortogonais, no caso do BB84, ou estados entrelaçados, no caso do E91, permitem a geração secreta de uma chave aleatória através da qual os usuários legítimos podem realizar uma comunicação privada completamente segura.

Conforme Gao *et al*. (2008) a comunicação quântica segura direta (*quantum secure direct communication* - QSDC) é outro ramo da criptografia quântica que atraiu muita atenção como um possível substituto para a distribuição quântica de chaves, no qual duas entidades de comunicação trocam mensagens clássicas seguras sem estabelecer previamente nenhuma chave compartilhada. A QSDC permite que o emissor (tradicionalmente chamado de Alice) transmita diretamente a mensagem, e não uma chave aleatória ao receptor (tradicionalmente chamado de Bob), de uma maneira determinística e segura. Um protocolo de QSDC cuidadosamente concebido teoricamente também pode apresentar segurança incondicional (DENG; LONG, 2004; DENG, *et al*., 2006).

Apesar dos avanços teóricos e experimentais, ao contrário da QKD, os esquemas ópticos para realização de QSDC ainda não estão comercialmente disponíveis. Isso acontece porque os protocolos propostos na literatura exigem alguns recursos quânticos que não estão disponíveis com a tecnologia de hoje, principalmente memória quântica. Assim, novos protocolos que não necessitem de memória quântica e que possam utilizar estados coerentes são de grande interesse. Nesta direção, a presente tese apresenta três novos esquemas ópticos para QSDC que não requerem memória quântica e que utilizam estados coerentes atenuados. Os protocolos de QSDC propostos utilizam a distribuição espectral das fontes luminosas e moduladores de fase dependentes da frequência para aumentar a segurança. Além disso, o primeiro esquema óptico executa QSDC e QKD ao mesmo tempo, o segundo protocolo utiliza estados térmicos para aumentar a segurança e o terceiro esquema faz QSDC de um sinal analógico.

Um ponto importante no projeto de sistemas de comunicação quântica em redes ópticas é a detecção de fótons. O tipo de detector de fótons mais comum e que pode ser

encontrado comercialmente é o detector de fótons baseado em fotodiodo de avalanche (APD). Estes detectores são caros e possuem várias restrições de funcionamento: 1) Operam com altas voltagens (40V-300V) e, por isso, possuem um tempo de vida útil menor; 2) Necessitam de resfriamento para reduzir a contagem de escuro, o que aumenta o consumo de energia do equipamento. 3) Possuem restrição de velocidade de operação devido ao fenômeno de *afterpulsing*[1]. Por outro lado, fotodiodos PIN são mais baratos, não precisam ser resfriados, operam com baixa voltagem (5V-10V) e são mais velozes que o APD. Entretanto, o fotodiodo PIN não possui o mecanismo de ganho do APD. Ou seja, no PIN um fóton absorvido gera apenas um elétron. Uma forma de resolver este problema e detectar fótons utilizando fotodiodos PIN é realizar a detecção homódina (ou heteródina) do fóton. Neste caso, os fótons do oscilador local complementam o sinal. Com este objetivo, de aproveitar o fotodiodo PIN, este trabalho apresenta os resultados experimentais da detecção homódina de estados coerentes fortemente atenuados. Esse experimento mostrou que um sinal analógico transportado por um estado coerente fortemente atenuado pode ser recuperado por um receptor óptico baseado em PIN.

Por fim, a polarização da luz é uma importante propriedade que pode ser usada para testar princípios fundamentais da física, ou pode ainda ser usada como portadora de informação em sistemas de comunicação ou computação quântica. Em todos os exemplos de uso da polarização quântica encontrados na literatura, somente luz completamente polarizada é considerada. Entretanto, não é uma tarefa trivial manter a luz completamente polarizada, uma vez que a polarização diminui ou mesmo desaparece após a propagação da luz em meios com variação aleatória de birrefringência ou em meios cuja birrefringência depende da frequência. Este último caso é bem importante, pois qualquer fonte luminosa produz luz com distribuição espectral. Para estes pulsos de luz, cada componente espectral experimenta uma transformação diferente no canal. Portanto, após a propagação, cada componente espectral terá uma polarização diferente. Assim, é importante entender como o grau de polarização da luz varia quando esta se propaga por diferentes tipos de canais. Nesta direção, esta tese mostra como calcular o grau de polarização de estados contínuos coerentes e de um fóton, bem como analisa a despolarização devido à distribuição espectral. Por fim, resultados experimentais da estimação do grau de polarização através da medição da visibilidade de polarização são apresentados.

---

[1] Produção de pulsos devido a elétrons que estavam aprisionados na rede cristalina e ao escaparem são acelerados produzindo uma avalanche, fotocorrente falsa, pois não foi produzida devido ao fóton inicial.

A presente tese está estruturada da seguinte forma: Na seção 2 foi feito uma revisão sobre criptografia para contextualizar os problemas de uma comunicação segura. Na seção 3 são abordados os principais protocolos estudados para a distribuição quântica de chaves. Na seção 4 tem-se uma breve explanação sobre os estados quânticos da luz. Na seção 5 três protocolos de comunicação quântica segura direta são apresentados. Na seção 6 o experimento de detecção homódina de fótons é descrito. Na seção 7 a nova medida do grau de polarização e o cálculo do grau de polarização de estados contínuos de um fóton e coerente são apresentados. Na seção 8 o experimento para estimar o grau de polarização através da visibilidade de polarização é descrito. Por fim, a seção 9 traz as conclusões e perspectivas de trabalhos futuros.

2 CRIPTOGRAFIA

2.1 Criptografia Clássica

Desde os primórdios da civilização o Homem sempre se deparou com o problema de transmitir secretamente informações importantes. A ciência que estuda essa arte de se comunicar confidencialmente, tendo a certeza de que somente as partes interessadas terão acesso à informação, recebe o nome de criptografia (RIGOLIN; RIEZNIK, 2005). Em outras palavras, conforme Gisin *et al.* (2002), a criptografia é a arte de tornar uma mensagem ininteligível para qualquer parte não autorizada. Basicamente, a criptografia consiste de um conjunto de regras que visam codificar a informação de forma que só o emissor e o receptor consigam decifrá-la. Para isso existem varias técnicas que têm sido modificadas e aperfeiçoadas para aumentar a segurança.

Com os avanços tecnológicos vieram a interconectividade e a comodidade de resolver problemas diversos via internet. Quando informações pessoais, financeiras e militares são transferidas através das redes de comunicações, elas tornam-se vulneráveis às técnicas de monitoramento por adversários e, potencialmente, podem ter consequências até catastróficas. Estes problemas podem ser evitados através da encriptação da informação de forma que esta se torne ininteligível a todos, menos ao destinatário. Na forma mais básica de criptografia, este objetivo pode ser atingido se somente o remetente e o destinatário autorizados possuírem uma sequência aleatória de bits, conhecida como chave, que é usada para encriptação pelo remetente e decriptação pelo destinatário. Para que um sistema de criptografia seja seguro, segundo Brassard (1988) deve ser impossível decifrar a mensagem criptografada sem a chave. Ou seja, dada uma chave, todas as mensagens possíveis são igualmente prováveis. Na prática, a segurança de um sistema criptográfico depende dos detalhes matemáticos (o tipo de função de encriptação/decriptação utilizada) e tecnológicos (a implementação em hardware).

Por fim, embora a confidencialidade seja a aplicação tradicional da criptografia, ela também é utilizada para alcançar outros objetivos como, por exemplo, autenticação, assinaturas digitais, compromisso de informação e o não-repúdio. Este último visa garantir que o autor de uma mensagem não possa negar tê-la criada e/ou assinada.

Nesta seção, o objetivo é apresentar de forma sucinta a criptografia simétrica e a criptografia assimétrica.

2.2 Criptografia Simétrica

A técnica de criptografia simétrica usa a mesma chave, ou seja, tanto o emissor quanto o receptor da mensagem compartilham uma chave secreta, que é usada na encriptação e decriptação do que é transmitido. Porém, o problema fundamental neste tipo de criptografia está em como transmitir de forma segura a chave entre emissor e receptor, já que há o risco de interceptação. Além disso, os algoritmos simétricos ou de chave privada são feitos de forma que impossibilite a criptoanálise (obtenção da mensagem encriptada sem a chave) em tempo hábil. É importante fazer com que a mensagem encriptada pareça o mais aleatória possível, sem padrões repetitivos e redundâncias, de forma que a única alternativa acaba sendo testar todas as chaves possíveis. A presença de padrões ou frequência de símbolos pode identificar a chave ou reduzir o número de tentativas de encontrá-la. Por isso, uma maior segurança é obtida se a chave é utilizada apenas uma vez.

Para Alice enviar uma mensagem a Bob (os nomes convencionais para o transmissor e para o receptor, respectivamente), neste esquema, Alice criptografa sua mensagem, uma sequência de bits denotada por M_1, usando uma chave k gerada aleatoriamente. A encriptação usando a função *xor* consiste simplesmente em adicionar (módulo 2) cada bit da mensagem ao bit correspondente da chave: $S = M_1 \oplus k$, sendo que $\oplus$ denota a adição módulo 2). Em seguida, a sequência de bits S é enviada para Bob, que decripta a mensagem, fazendo uma nova adição módulo 2 da mensagem encriptada com a chave subtraindo a chave: $S \oplus k = M_1 \oplus k \oplus k = M_1$. Este protocolo de criptografia simétrica usando a função xor é perfeitamente seguro se chave e mensagem possuem o mesmo tamanho e a chave é utilizada apenas uma vez, daí o nome de *one time pad*.

Devido à função *xor*, como os bits do texto encriptado são tão aleatórios quanto os da chave, eles não contêm nenhuma redundância que possa ser utilizada por um espião. Entretanto, como Alice e Bob devem possuir a mesma chave, a chave tem que ser transmitida (de um deles para o outro) por um meio confiável, como um mensageiro confiável ou através de uma reunião pessoal entre Alice e Bob. Este procedimento pode ser complexo e caro. Devido ao problema de distribuir sequências longas de bits de chave, o *one time pad* é usado

apenas para as aplicações mais críticas. Uma alternativa segura para resolver o problema da distribuição da chave no protocolo de criptografia simétrica é a distribuição quântica de chaves, como será visto mais adiante.

2.3 Criptografia Assimétrica

A diferença fundamental entre a criptografia simétrica e a assimétrica é que nesta última as operações de encriptação e decriptação usam chaves distintas. A descoberta da criptografia assimétrica, também chamada criptografia de chave pública, foi o maior avanço em criptografia em séculos (STANTON, 2000).

Nos algoritmos assimétricos ou de chave pública, cada participante da comunicação possui uma chave privada *D*, que somente ele conhece, e uma chave pública *E*, que qualquer pessoa pode acessar. Esta chave normalmente fica armazenada em um local capaz de garantir que aquela chave está associada apenas a uma pessoa. Uma chave funciona como a inversa da outra,

$$K_D\left(K_E\left(M\right)\right) = K_E\left(K_D\left(M\right)\right) = M, \tag{2.1}$$

onde K_x é a função criptográfica K associada à chave x. Na verdade, sabendo-se uma chave é possível chegar à outra, já que as duas são inversas, entretanto, essa operação deve ser bastante custosa em termos de recurso e/ou tempo, para que o protocolo seja seguro. É desejável que o processo inverso seja tão custoso quanto testar todas as possibilidades. Os dois principais objetivos da criptografia assimétrica são:

1) Envio de mensagens confidenciais:

   – uma pessoa *A* pode utilizar a chave pública de *B* para enviar uma mensagem confidencial que somente *B* pode decodificar com sua chave privada. Isto resolve o problema de enviar a chave na criptografia simétrica; basta utilizar a chave pública, que não é secreta.

2) Envio de mensagens autenticadas:

– uma pessoa *B* pode utilizar sua chave privada para encriptar uma mensagem de forma a garantir que ele a escreveu. Neste caso, o objetivo não é esconder a mensagem, e sim autenticá-la, uma vez que qualquer um pode decodificar a mesma com a chave pública de *B*.

Diffie e Hellman (1976) propuseram a criptografia assimétrica pela primeira vez e segundo os mesmo é uma alternativa que impede o tráfego da própria chave pelo meio compartilhado. A primeira implementação real foi então desenvolvida por Ronald Rivest, Adi Shamir e Leonard Adleman em 1978. Este é conhecido como protocolo RSA em homenagem aos seus criadores e que, até o momento, é a forma mais usada de criptografia assimétrica. O sistema explora a propriedade de certas operações matemáticas que são mais simples de serem efetuadas em um sentido do que no sentido oposto, ou seja, é fácil de calcular a função $y = f(x)$, mas é difícil dado x encontrar y. Em outras palavras, a segurança dos protocolos criptográficos de chave pública, incluindo o RSA, baseia-se na complexidade computacional. No contexto de complexidade computacional, a palavra difícil, significa que o tempo necessário para executar uma tarefa cresce exponencialmente com o número de bits na entrada, enquanto fácil, significa que ele cresce polinomialmente.

A segurança do RSA é baseada na fatoração de grandes números inteiros. Apesar de sua elegância, esta técnica possui um problema. Ainda não foi possível provar se o problema de fatorar números inteiros é realmente "difícil" ou não. Isto implica que, no âmbito da computação clássica, a existência de um algoritmo rápido para a fatoração não pode ser descartada. Além disso, a descoberta em 1994 por Peter Shor de um algoritmo quântico que permite a rápida fatoração de números inteiros, ou seja, em tempo polinomial, põe em xeque o uso do RSA.

O método empregado no RSA usa a função totiente, introduzida pelo matemático e físico suíço Leonhard Euler que fornece o número de inteiros positivos menores que n, que são primos com n. Esta função apresenta a propriedade de que, para dois números m e n primos entre si, $M^{\phi(n)} \bmod(n) = 1$, onde $x \bmod(y)$ deve ser entendido como o resto da divisão de x por y e $\phi(n)$ é a função totiente de Euler. Em particular, quando n é produto de dois números primos p e q, sabe-se que $\phi(n) = (p-1)\cdot(q-1)$.

Primeiramente, um usuário gera um par de chaves $(e,\ n)$, como chave pública, e $(d,\ n)$ como chave privada, sendo que $n = p \cdot q$ (p e q são números primos muito grandes). Além disso, d é um número muito grande primo relativo a $\phi(n)$ e e é o inverso multiplicativo do primeiro, sendo, portanto, um número pequeno $e \cdot d \equiv 1 \pmod{\phi(n)}$.

Por fim, uma mensagem M é encriptada em uma cifra C conforme a fórmula $C = M^e \bmod(n)$, enquanto a decriptação segue $M = C^d \bmod(n)$. Com isto, $M = \left(M^e\right)^d \bmod(n) = M^{ed} \bmod(n) = M^{ed} \bmod(\phi(n)) = M$.

O ponto chave para quebrar este algoritmo é a obtenção de $\phi(n)$, seja a partir de n, ou a partir de p e q após a fatoração de n; ambas as técnicas são extremamente custosas, tendo em vista que o melhor método conhecido para fatoração de inteiros possui complexidade $O\left(ln(n)^{(ln(n)/ln(ln(n)))^{1/2}}\right)$ (RIVEST *et al*. 1978), impossibilitando a fatoração de um número de 128 bits, por exemplo, em tempo hábil.

Até agora, ninguém provou a existência de qualquer função unidirecional que revelasse o valor de um dos fatores primo. Em outras palavras, a existência de criptossistemas assimétricos seguros não é comprovada. Isso representa uma séria ameaça para esses criptossistemas. Em uma sociedade como a atual, onde a informação e a comunicação segura são de extrema importância, não se pode tolerar tal ameaça. Por exemplo, uma descoberta noturna pela Matemática poderia tornar o dinheiro eletrônico imediatamente sem valor. Para limitar tais riscos econômicos e sociais, não há alternativa senão recorrer a criptossistemas simétricos. A Criptografia Quântica, em particular a distribuição quântica de chaves, tem um papel a desempenhar em tais sistemas alternativos (GISIN *et al.*, 2002).

3 DISTRIBUIÇÃO QUÂNTICA DE CHAVES - QKD

A Distribuição Quântica de Chave (QKD - *Quantum Key Distribution*) é a mais maduras das técnicas de comunicação quântica. Dois usuários remotos podem usar a QKD para criar uma chave privada com segurança. Essas chaves podem então ser usadas em um esquema criptográfico simétrico, como o *one time pad* descrito na sessão 2.2. O objetivo desta seção é apresentar de forma sucinta a distribuição quântica e chaves (QKD).

Conforme Brassard *et al*. (2000), para ser prático e seguro, um esquema QKD deve ser baseado em tecnologia existente ou quase existente, mas sua segurança deve ser garantida contra um espião com poder limitado apenas pelas leis da mecânica quântica. Nos protocolos de QKD a informação é codificada em estados quânticos e, basicamente, três características garantem a segurança: 1) O uso de estados quânticos não ortogonais. 2) Escolha aleatória do estado quântico a ser enviado e/ou da base de medição. 3) O teorema da não clonagem. Este último pode ser demonstrado da seguinte maneira: Seja uma máquina de clonagem representada pelo operador unitário U. Então $U|a\rangle|0\rangle = |a\rangle|a\rangle$ e $U|b\rangle|0\rangle = |b\rangle|b\rangle$. Portanto $\langle a|\langle a|b\rangle|b\rangle = \langle a|b\rangle^2 = \langle a|\langle 0|U^{\dagger}U|0\rangle|b\rangle = \langle a|b\rangle\langle 0|0\rangle = \langle a|b\rangle$. Entretanto $\langle a|b\rangle^2 = \langle a|b\rangle$ se somente se $\langle a|b\rangle = 1$ ($|a\rangle$ e $|b\rangle$ são os mesmos estados quânticos) ou $\langle a|b\rangle = 0$ ($|a\rangle$ e $|b\rangle$ são ortogonais). Portanto, não é possível construir uma máquina de clonagem universal.

Há muitos protocolos de QKD, nesta seção uma breve revisão dos protocolos BB84, B92 e DPS são apresentados.

3.1 Protocolo BB84

O protocolo BB84 foi primeiramente proposto por Bennett e Brassard (1984) e ele utiliza dois pares de estados quânticos ortogonais. Considerando a polarização da luz de um fóton, têm-se no espaço de Hilbert H^2 as bases retilínea $B_R = \{|H\rangle, |V\rangle\}$ e diagonal $B_D = \{|+\rangle = (|H\rangle + |V\rangle)/2^{1/2}, |-\rangle = (|H\rangle - |V\rangle)2^{1/2}\}$. Os estados dentro de uma base são ortogonais entre si enquanto que estados de bases diferentes são não ortogonais: $\langle H|+\rangle = \langle H|-\rangle = \langle V|+\rangle = \langle V|-\rangle = 1/2^{1/2}$. Além disso, os estados $|H\rangle$ e $|+\rangle$ representam o bit lógico ‘0’ enquanto que os estados $|V\rangle$ e $|-\rangle$ representam o bit lógico ‘1’. O protocolo é como mostrado a seguir:

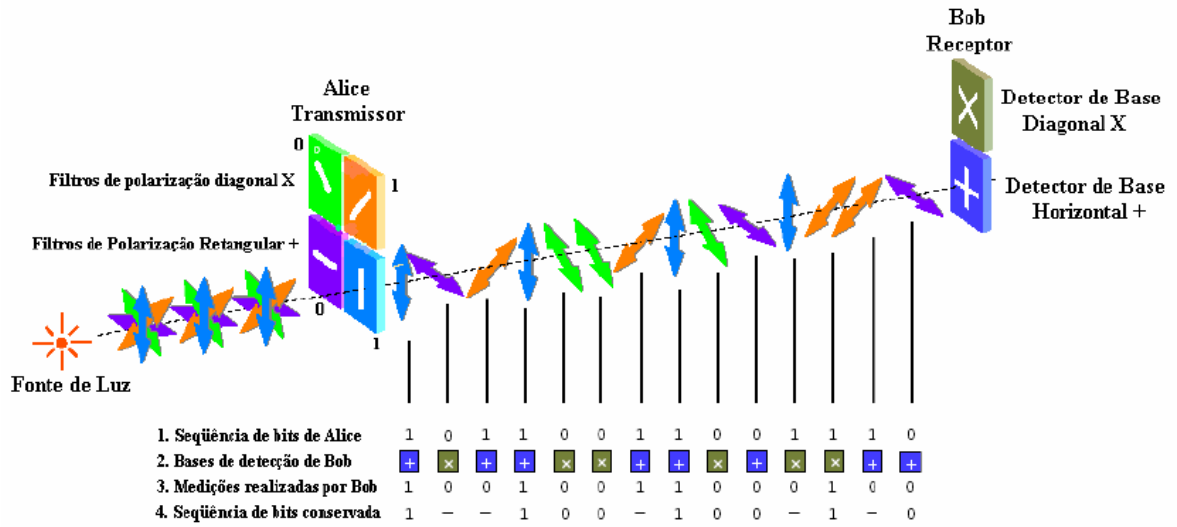
1) Alice escolhe de forma aleatória a base B_R ou B_D e o estado quântico dentro da base. Então Alice prepara um fóton no estado quântico escolhido e o envia para Bob.

2) Bob escolher aleatoriamente uma base de medição B_R ou B_D para medir o estado quântico enviado por Alice.

3) Alice e Bob divulgam publicamente as bases utilizadas. Nos casos em que eles usaram a mesma base, os valores dos bits enviado por Alice e medido por Bob devem ser os mesmos e, portanto, este bit é utilizado na chave. Quando Alice e Bob escolhem bases diferentes, há uma probabilidade de 50% do bit enviado por Alice ser diferente do Bit medido por Bob. Neste caso, o bit é descartado.

4) Depois que todos os bits resultantes de situações nas quais bases diferentes foram utilizadas forem descartados, a sequência de bits restantes forma a chave 'crua'. Um protocolo de correção de erros é utilizado para fazer a reconciliação das sequências binárias de Alice e Bob e, por fim, a amplificação de privacidade é realizada para diminuir o possível conhecimento de uma parte da chave por uma espiã. A FIGURA 1 a seguir ilustra o protocolo.

Figura 1 – Princípio da distribuição quântica de chaves, usando polarização da luz, de acordo com o protocolo BB84.



Fonte: adaptada de Zbinden, H. *et al.* (1998).

Caso a comunicação tenha sido interceptada por Eve, a espiã, Bob detectará inconsistências em suas medições (bits diferentes dos correspondentes de Alice). A probabilidade de Eve causar um erro na comunicação entre Alice e Bob é de 25% por fóton

enviado: 50% de probabilidade de Eve medir o qubit em uma base diferente da usada por Alice e Bob, e 50% de probabilidade do bit enviado por Eve causar um erro em Bob. Assim, quando Eve intercepta a comunicação, na ausência de ruídos inerentes ao sistema, ela acabará por tornar, em média, $1/4$ dos bits de Alice e Bob diferentes, revelando assim sua presença. Sob estas condições, a chave será descartada e o processo reiniciado. A TABELA 1 a seguir mostra um exemplo da realização do BB84.

Tabela 1 – Realização do protocolo de QKD BB84.

Transmissão Quântica													
Bits aleatórios de Alice													
1	0	0	1	1	0	1	0	0	0	1	1	0	1
Bases aleatórias de Alice													
R	*D*	*R*	*R*	*D*	*D*	*R*	*D*	*R*	*D*	*D*	*R*	*D*	*D*
Fótons polarizados enviados por Alice													
$\|V\rangle$	$\|+\rangle$	$\|H\rangle$	$\|V\rangle$	$\|-\rangle$	$\|+\rangle$	$\|V\rangle$	$\|+\rangle$	$\|H\rangle$	$\|+\rangle$	$\|-\rangle$	$\|V\rangle$	$\|+\rangle$	$\|-\rangle$
Bases aleatórias de Bob													
D	*D*	*R*	*D*	*R*	*D*	*R*	*R*	*D*	*R*	*D*	*R*	*D*	*R*
Bits recebidos por Bob													
1	0	0		1	0	1	0	1		1	1	0	
Bob comunica as bases que recebeu bits													
D	*D*	*R*		*R*	*D*	*R*	*R*	*D*		*D*	*R*	*D*	
Alice comunica quais bases estão corretas													
	Ok	Ok			Ok	Ok				Ok	Ok	Ok	
Alice e Bob revelam seus bits (se não houver espião)													
	0	0			0	1				1	1	0	
Bob revela alguns bits aleatoriamente													
		0				1					1		
Alice confirmam os bits													
		Ok				Ok					Ok		
Chave final													
	0				0					1		0	

Fonte: adaptada de Bennett e Brassard (1984).

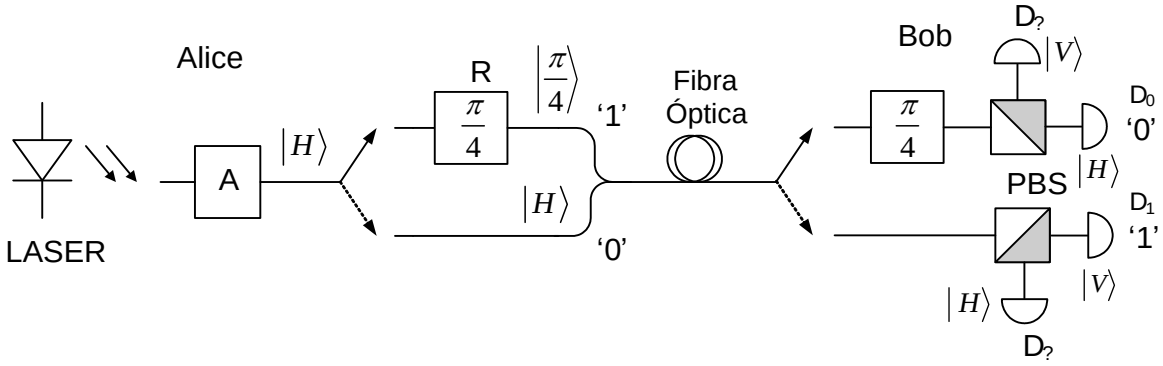
É importante notar que Alice divulga apenas as bases da sequência enviada por ela, os bits equivalentes não são divulgados. Para ver se a distribuição foi segura, após a filtragem das bases, eles comparam uma parte dos bits da chave, bits de sacrifício, e computam a taxa de erro. É de se esperar, nos casos em que Bob e Alice utilizaram a mesma base, que eles obtenha o mesmo bit. Porém, normalmente, alguns bits podem ser invertidos durante a transmissão ou por ruído na medição. Por conta dessas circunstâncias, há uma esperada taxa de erro que depende da qualidade do canal, do transmissor, dos moduladores e do detector. Essa taxa de erro é chamada QBER (*quantum bit error rate*). Se a taxa de erro estimada for maior do que 11% pode-se concluir que houve uma fonte externa de erro na transmissão, provavelmente devido à presença de um espião. Caso contrário, a comunicação está segura o suficiente e os restantes dos bits poderão ser usados como chave criptográfica. Durante este processo, um espião pode eventualmente extraviar alguma informação. Assim, objetivando aumentar a privacidade, Alice e Bob aplicam em suas chaves uma função Hash. A aplicação dessa função embaralha os bits da chave de tal modo que, mesmo para o caso das duas chaves possuírem apenas um bit diferente, as chaves finais apresentarão, aproximadamente, 50% dos valores dos bits diferentes.

3.2 Protocolo B92

Em 1992 Charles Bennett propôs um protocolo para QKD utilizando apenas dois estados não ortogonais. Este protocolo é conhecido pelo nome B92 ou protocolo de dois estados. Para descrever o B92 utilizamos as mesmas notações utilizadas para a descrição do protocolo BB84. Alice prepara aleatoriamente cada fóton com polarização horizontal $|H\rangle$ ou diagonal (45°) $|+\rangle$. Para a polarização $|H\rangle$ atribui-se o valor de bit de 0 e à polarização $|+\rangle$ um valor de bit de 1. Alice envia uma sequência de pulsos polarizados para Bob que está equipado com um analisador de polarização e um único detector de fótons. Para cada fóton que chega, Bob ajusta aleatoriamente suas bases de medições, R $\{|H\rangle,|V\rangle\}$ e D $\{|+\rangle,|-\rangle\}$. Se Bob detectar o fóton enviado por Alice, ele saberá com certeza a polarização e, portanto, o valor do bit ‘ 0 ’ ou ‘1’ enviado. Se Bob detectar um fóton ao medir na base *R*, ele saberá que Alice enviou um fóton com polarização de $|+\rangle$, portanto bit ‘1’. Se Bob detectar um fóton ao medir na base *D,* ele saberá que Alice enviou um fóton com polarização de $|H\rangle$, portanto, bit ‘0’. Assim, Bob atribui a detecções na base *R* o valor de bit de ‘1’ e detecções na base *D*, o valor de bit ‘ 0 ’. Se Bob não detectar nenhum fóton ele não poderá estar certo sobre qual

estado Alice enviou. Assim, Alice e Bob mantêm apenas os resultados daquelas medições onde Bob detectou um fóton. Esta sequência de bits forma a chave. O esquema óptico que implementa o B92 com polarização pode ser visto na FIGURA 2. A TABELA 2 mostra o procedimento do protocolo B92.

Figura 2 – Esquema óptico para realização do protocolo B92: *A* – atenuador variável, *R* – rotacionador de polarização e *PBS* – divisor de feixes por polarização.



Fonte: adaptada de Mendonça (2006).

Tabela 2 –Realização do protocolo de QKD B92.

Alice		**Bob**			
Polarização	**Bit**	**Base**	**Detector 2**	**Detector 1**	**Bit**
$\|H\rangle$	0	*R*	**100%** $\|H\rangle$	**0%**	
		D	**50%** $\|+\rangle$	**50%** $\|-\rangle$	**0**
$\|+\rangle$	1	*R*	**50%** $\|H\rangle$	**50%** $\|V\rangle$	**1**
		D	**100%** $\|+\rangle$	**0%**	

Fonte: elaborada pelo autor.

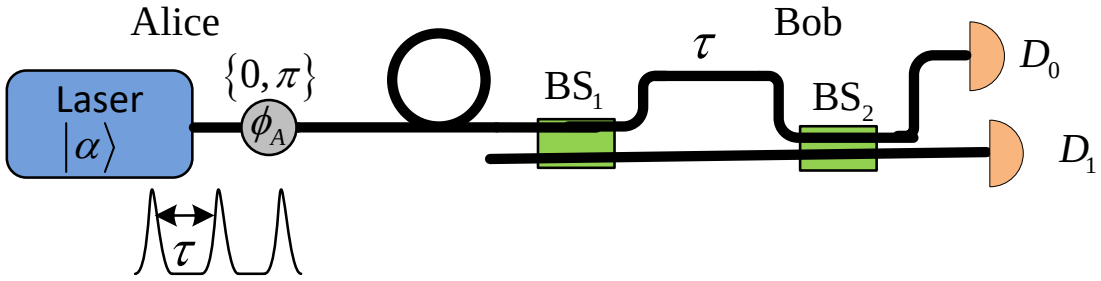
Após se comunicarem publicamente para determinar em quais instantes de tempo fótons foram detectados por Bob, Alice e Bob informam uma parte de seus bits para a estimação da taxa de erro e depois são descartados. A chave final é obtida, assim como no protocolo BB84, após correção de erros e amplificação de privacidade.

3.3 Protocolo – DPS-QKD (Differential Phase-Shift Quantum Key Distribution)

Nos protocolos de QKD com deslocamento diferencial de fase, Alice envia para Bob uma sequência de pulsos (estados coerentes) fortemente atenuados ($\langle n \rangle \sim 0{,}1$) sendo que, cada pulso que sai de Alice tem a fase aleatoriamente modulada de ‘0’ ou ‘ π’. Como a potência do sinal transmitido é muito baixa, a probabilidade de haver dois ou mais fótons no mesmo pulso é muito pequena.

Enquanto em Alice existem apenas o laser e o modulador de fase, em Bob há um interferômetro Mach-Zehnder que possui um braço longo e outro curto, sendo o atraso temporal experimentado pelo pulso no braço longo, τ, igual ao intervalo de tempo entre dois pulsos consecutivos enviados por Alice. O esquema é mostrado na FIGURA 3. Por causa dessa diferença de tamanho dos braços do interferômetro, a interferência em BS_2 ocorre entre pulsos adjacentes.

Figura 3 – Esquema óptico para realização do protocolo DPS-QKD. $BS_{1,2}$ – divisor de feixes; ϕ_A - modulador de fase de Alice; $D_{0,1}$ - detectores de fótons.



Fonte: adaptada de Damasceno (2017).

Para mostrar o funcionamento do protocolo, começamos pela definição do operador unitário que modela o divisor de feixes, U_{BS}. Se dois estados coerentes, $|\alpha\rangle$ e $|\beta\rangle$, chegam nas entradas do divisor de feixes ao mesmo tempo e com a mesma polarização, então os estados coerentes nas saídas do divisor de feixes serão:

$$U_{BS}\left|\alpha,\beta\right\rangle = \left|\left(\alpha+\beta\right)/\sqrt{2}\right\rangle\left|\left(-\alpha+\beta\right)/\sqrt{2}\right\rangle. \tag{3.1}$$

Usando (3.1) no esquema óptico da FIGURA 3, chega-se à seguinte expressão para o resultado da interferência em BS_2 entre os pulsos *n*-1 e *n*:

$$U_{BS_2}\left|\frac{\alpha}{\sqrt{2}}e^{i\phi_A^{n-1}}\right\rangle\left|\frac{\alpha}{\sqrt{2}}e^{i\phi_A^{n}}\right\rangle = \\ =\left|\sqrt{2}\alpha e^{i(\phi_A^{n-1}+\phi_A^{n})}\cos\left(\frac{\phi_A^{n-1}-\phi_A^{n}}{2}\right)\right\rangle_0\left|-\sqrt{2}\alpha e^{i(\phi_A^{n-1}+\phi_A^{n})}\sin\left(\frac{\phi_A^{n-1}-\phi_A^{n}}{2}\right)\right\rangle_1. \tag{3.2}$$

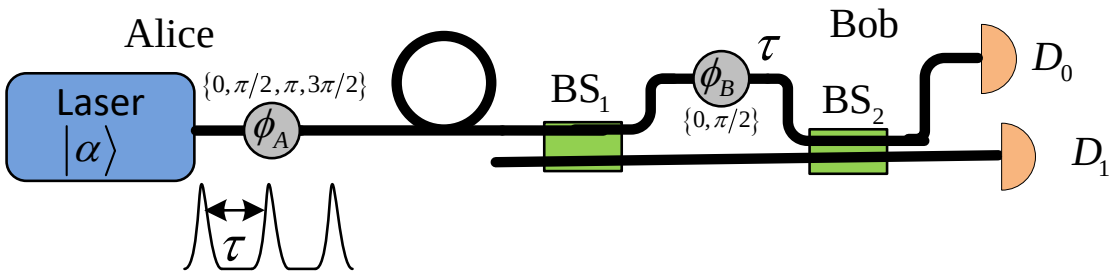
Na equação (3.2), os subíndices ‘0’ e ‘1’ indicam as portas de saída do BS. Assim, os fótons são detectados de acordo com a diferença de fase entre os pulsos interferentes *n* e *n*-1: se $\phi_A^{n-1}-\phi_A^{n}=0$, poderá haver detecção em D_0, significando, em caso de detecção, que um bit ‘0’ foi registrado; Por outro lado, se $\phi_A^{n-1}-\phi_A^{n}=\pi$ poderá haver detecção em D_1, significando que um bit ‘1’ foi registrado.

Após a fase de detecções, Bob informa para Alice, através de um canal clássico, em quais instantes de tempo houve detecção de fótons. De posse dessa informação e dos valores de modulação de fase utilizados, Alice consegue saber em quais detectores Bob teve detecção e, portanto, o valor de bit registrado por ele. Na ausência de ruídos, Alice e Bob obtêm uma sequência idêntica de bits.

O protocolo DPS-QKD além de requerer um sistema óptico mais simples que o BB84, ele também é mais eficiente, pois todos os fótons detectados contribuem para a formação da chave.

Uma variante do DPS-QKD é o protocolo de distribuição quântica de chaves com deslocamento diferencial de fase em quadratura, DQPS-QKD. O esquema óptico que implementa o DQPS-QKD pode ser visto na FIGURA 4.

Figura 4 – Esquema óptico para realização do protocolo DQPS-QKD. BS - divisor de feixes; ϕ_A - modulador de fase de Alice; ϕ_B - modulador de fase de Bob; $D_{0,1}$ – detectores de fótons.



Fonte: adaptada de Damasceno (2017).

Como se pode observar na FIGURA 4, agora Bob também possui um modulador de fase. As fases utilizadas (escolhidas aleatoriamente) por Alice são {0, π/2, π, 3π/2}, enquanto Bob utiliza apenas as fases (escolhidas aleatoriamente) {0, π/2}. Portanto, os estados que chegam ao BS$_2$ na FIGURA 4 são:

$$\cdots \underbrace{\left|\frac{\alpha}{\sqrt{2}}e^{i\phi_A^n}\right\rangle_S \left|\frac{\alpha}{\sqrt{2}}e^{i\left(\phi_A^{n-1}+\phi_B^{n-1}\right)}\right\rangle_L}_{n} \cdots \underbrace{\left|\frac{\alpha}{\sqrt{2}}e^{i\phi_A^3}\right\rangle_S \left|\frac{\alpha}{\sqrt{2}}e^{i\left(\phi_A^2+\phi_B^2\right)}\right\rangle_L}_{3}$$
$$\otimes \underbrace{\left|\frac{\alpha}{\sqrt{2}}e^{i\phi_A^2}\right\rangle_S \left|\frac{\alpha}{\sqrt{2}}e^{i\left(\phi_A^1+\phi_B^1\right)}\right\rangle_L}_{2} \underbrace{\left|\frac{\alpha}{\sqrt{2}}e^{i\phi_A^1}\right\rangle_S}_{1} |0\rangle_L . \tag{3.3}$$

Em (3.3), ϕ_A^K e ϕ_B^K representam, respectivamente, os valores de fase escolhidos por Alice e Bob, respectivamente, no k-ésimo instante de tempo. A interferência se dá entre os pulsos vindos dos braços curto e longo que chegam no divisor BS$_2$ ao mesmo tempo e com a mesma polarização. Assim, os estados depois de BS$_2$ são:

$$\left|\frac{\alpha}{2}e^{i\phi_A^1}\right\rangle_0\left|\frac{\alpha}{2}e^{i\phi_A^1}\right\rangle_1$$

$$\left|\alpha e^{i\left(\frac{\phi_A^1+\phi_A^2+\phi_B^1}{2}\right)}\cos\left(\frac{\phi_A^1+\phi_B^1-\phi_A^2}{2}\right)\right\rangle_0\left|-i\alpha e^{i\left(\frac{\phi_A^1+\phi_A^2+\phi_B^1}{2}\right)}\sin\left(\frac{\phi_A^1+\phi_B^1-\phi_A^2}{2}\right)\right\rangle_1$$

$$\left|\alpha e^{i\left(\frac{\phi_A^2+\phi_A^3+\phi_B^2}{2}\right)}\cos\left(\frac{\phi_A^2+\phi_B^2-\phi_A^3}{2}\right)\right\rangle_0\left|-i\alpha e^{i\left(\frac{\phi_A^2+\phi_A^3+\phi_B^2}{2}\right)}\sin\left(\frac{\phi_A^2+\phi_B^2-\phi_A^3}{2}\right)\right\rangle_1 \tag{3.4}$$

$$\vdots$$

$$\left|\alpha e^{i\left(\frac{\phi_A^{n-1}+\phi_A^n+\phi_B^{n-1}}{2}\right)}\cos\left(\frac{\phi_A^{n-1}+\phi_B^{n-1}-\phi_A^n}{2}\right)\right\rangle_0\left|-i\alpha e^{i\left(\frac{\phi_A^{n-1}+\phi_A^n+\phi_B^{n-1}}{2}\right)}\sin\left(\frac{\phi_A^{n-1}+\phi_B^{n-1}-\phi_A^n}{2}\right)\right\rangle_1 .$$

Observa-se em (3.4) que as detecções registradas quando $\phi_A^{n-1}+\phi_B^{n-1}-\phi_A^n$ é igual a ‘0’ ou ‘π’ são usadas para formar a chave enquanto as demais são descartadas. Para Bob, detecção em D_0 indica bit ‘0’ enquanto que detecção em D_1 indica bit ‘1’. Para Alice, tem-se a codificação mostrada na TABELA 3.

Tabela 3 – Codificação de Alice no protocolo DQPS-QKD.

$\phi_A^{n-1}-\phi_A^n$	ϕ_B^{n-1}	Bit de Alice
0	0	0
π	0	1
-π/2	π/2	0
π/2	π/2	1

Fonte: adaptada de Damasceno (2017).

Os fótons são detectados em D_0 ou D_1 de acordo com a diferença de fase entre os pulsos *n* e *n*-1: se a diferença de fase entre os pulsos consecutivos enviados por Alice for igual a 0 e Bob escolher $\phi_B = 0$, poderá haver detecção em D_0, indicando o bit ‘0’; se a diferença de fase entre os pulsos enviados por Alice for igual a π e Bob escolher $\phi_B = 0$ poderá haver detecção em D_1, indicando o bit ‘1’. Da mesma forma, se a diferença de fase entre os pulsos consecutivos enviados por Alice for igual a $-\pi/2$ e Bob escolher $\phi_B = \pi/2$, poderá haver detecção em D_0, indicando o bit ‘0’; Por outro lado, se a diferença de fase entre os pulsos enviados por Alice for igual a $\pi/2$ e Bob escolher $\phi_B = \pi/2$, poderá haver detecção em D_1,

indicando o bit ‘1’. No fim da fase de detecções do protocolo, Bob informa para Alice em quais instantes de tempo ele teve detecção e quais os valores de fase por ele usados a fim de que ela saiba quais bits precisam ser descartados. Em seguida vêm as etapas de estimação da taxa de erro utilizando uma parte da chave obtida, a correção de erros e a amplificação de privacidade.

4 ESTADOS QUÂNTICOS DA LUZ

4.1 Estado Número e Estados Coerente

O estado de número da luz, $|n\rangle$, é aquele que possui exatamente *n* fótons. Pois possui o número de fótons com a máxima precisão possível, a fase do estado número é totalmente aleatória. Além disso, o conjunto dos estados números $\{|0\rangle, |1\rangle, |2\rangle,...,|n\rangle,...\}$ forma uma base para o espaço de Hilbert de dimensão infinita. Ou seja, qualquer estado quântico da luz pode ser escrito como uma superposição (ou uma combinação linear) dos estados números.

O estado coerente, por sua vez, é o estado quântico mais próximo da descrição clássica. Os estados coerentes podem ser gerados usando o operador de Glauber $D(\alpha) = epx(\alpha a^{\dagger} - \alpha^{*} a)$ aplicado ao estado vácuo $|0\rangle$, o que define a expressão do estado coerente na base de estados números como sendo

$$\left|\alpha\right\rangle = e^{\left(\alpha a^{\dagger} - \alpha^{*} a\right)}\left|0\right\rangle = e^{\alpha a^{\dagger}} e^{\alpha^{*} a} e^{-|\alpha|^{2}/2}\left|0\right\rangle = e^{-\frac{|\alpha|^{2}}{2}} \sum_{n=0}^{\infty} \frac{\alpha^{n}}{\sqrt{n!}}\left|n\right\rangle. \tag{4.1}$$

Em (4.1) $a^{\dagger}$ e a são, respectivamente, os operadores criação ($a^{\dagger}|n\rangle = \sqrt{n+1}|n+1\rangle$) e aniquilação ($a|n\rangle = \sqrt{n}|n-1\rangle$). Algumas propriedades importantes dos estados coerentes são:

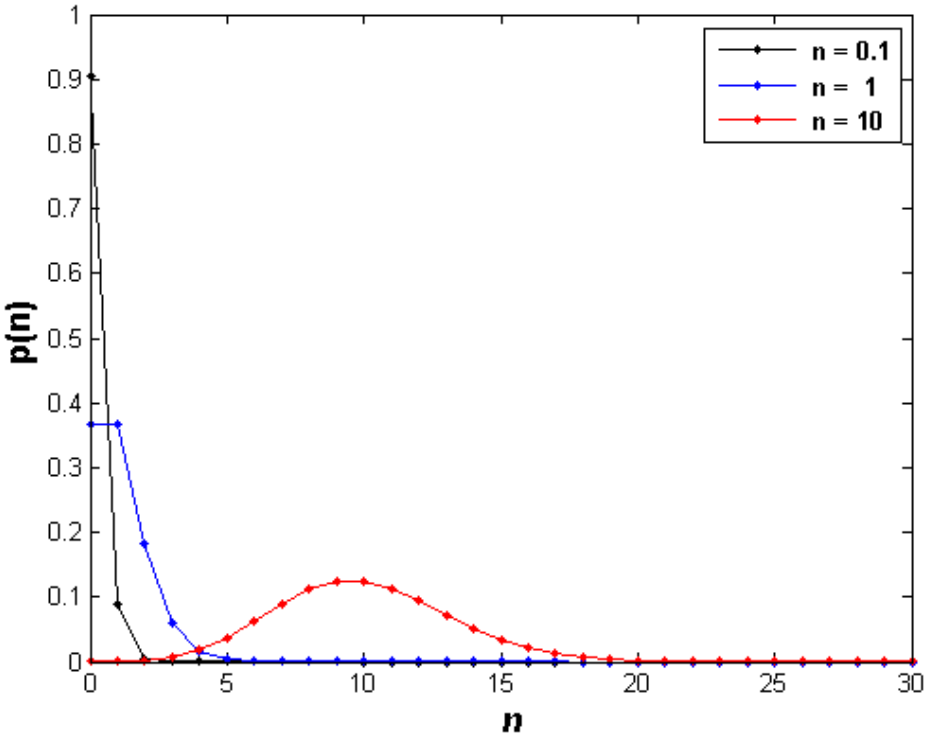
1) O número médio de fótons do estado $|\alpha\rangle$ é dado por $\langle n\rangle = \left\langle \alpha\middle| a^{\dagger} a \middle|\alpha\right\rangle = |\alpha|^{2}$.

2) A probabilidade de se encontrar *n* fótons em uma medição do número de fótons de $|\alpha\rangle$ é dado por:

$$p(n) = \left|\left\langle n \,|\, \alpha\right\rangle\right|^{2} = \frac{e^{-|\alpha|^{2}} \left(\left|\alpha\right|^{2}\right)^{n}}{n!}. \tag{4.2}$$

Ou seja, a distribuição do número de fótons do estado coerente é poissoniana. A FIGURA 5 mostra $p(n)$ versus n para três diferentes valores de $|\alpha|^2$ (0.1, 1 e 10).

Figura 5 – Distribuição do número de fótons $p(n)$ versus número de fótons n para estados coerentes com $|\alpha|^2$=0,1, $|\alpha|^2$=1 e $|\alpha|^2$=10.



Fonte: elaborada pelo autor.

3) O produto de incerteza é o mínimo permitido pelo princípio da incerteza de Heisenberg: $\Delta p \Delta q = h/4\pi$.

4) O conjunto de todos os estados coerentes $|\alpha\rangle$ é um conjunto supercompleto. A relação de completude para os estados coerentes que expressa esta propriedade é

$$\frac{1}{\pi}\int |\alpha\rangle\langle\alpha| d^2\alpha = 1. \tag{4.3}$$

5) Dois estados coerentes não ortogonais.

$$\left|\langle\alpha\,|\,\beta\rangle\right|^2 = \left|\exp\left[-\frac{1}{2}\left(|\,\alpha\,|^2 + |\,\beta\,|^2\right) + \beta\alpha^*\right]\right|^2 = \exp\left(-\left|\alpha-\beta\right|^2\right). \tag{4.4}$$

Entretanto, se a magnitude de $\alpha-\beta$ é muito maior que a unidade, os estados são aproximadamente ortogonais.

Os estados número e coerente descritos anteriormente são estados de um único modo, no sentido de que possuem uma única frequência. Obviamente, isso é uma simplificação do caso real, pois uma fonte que emitisse luz em uma única frequência violaria o princípio da incerteza de Heisenberg. Além disso, possuindo uma distribuição espectral, esta pode ser discreta ou contínua (SANTOS *et al*., 1997), ou ainda a versão discretizada da distribuição contínua (RAMOS, 2000). As versões discretizadas para estados contínuos de um fóton, dois fótons entrelaçados e estados coerentes são

$$\left|1_\omega\right\rangle = \int_0^\infty \sigma(\omega)\,\hat{a}^+(\omega)\,d\omega\left|0_\omega\right\rangle \approx \sum_{k=1}^{N}\sigma(k\omega_s)\sqrt{\omega_s}\left|0\right\rangle_1 ... \left|1\right\rangle_k ... \left|0\right\rangle_N = \sum_{k=1}^{N}\sigma(k\omega_s)\sqrt{\omega_s}\left|\tilde{1}\right\rangle_k, \tag{4.5}$$

$$\sum_{k=1}^{N}\left|\sigma(k\omega_s)\right|^2\omega_s = 1, \tag{4.6}$$

$$\left|2_\omega\right\rangle = \int_0^\infty d\Omega\sigma(\Omega)\frac{\left|\omega_0+\Omega,\omega_0-\Omega\right\rangle_{HH} + \left|\omega_0+\Omega,\omega_0-\Omega\right\rangle_{VV}}{\sqrt{2}} = \sum_{\substack{k,l=1\\k+l=M}}^{N}\sigma(k\omega_s,l\omega_s)\sqrt{\omega_s}\left[\frac{\left|\tilde{1}\right\rangle_k^H\left|\tilde{1}\right\rangle_l^H + \left|\tilde{1}\right\rangle_k^V\left|\tilde{1}\right\rangle_l^V}{\sqrt{2}}\right], \tag{4.7}$$

$$M\omega_s = 2\omega_0, \tag{4.8}$$

$$\left|\alpha_\omega\right\rangle = \exp\left[\int\left[\alpha(\omega)a^\dagger(\omega) - \alpha^*(\omega)a(\omega)\right]d\omega\right]\left|0_\omega\right\rangle = \prod_{k=1}^{N}\left|\alpha(k\omega_s)\sqrt{\omega_s}\right\rangle, \tag{4.9}$$

$$\langle n\rangle = \sum_{k=1}^{N}\left|\alpha(k\omega_s)\right|^2\omega_s. \tag{4.10}$$

Em (4.5) $|\sigma(\omega)|^2 d\omega$ dá a probabilidade da frequência do fóton único estar no intervalo (ω, $\omega + d\omega$). Além disso, em (4.5) – (4.10) ω_s é o passo de discretização no domínio da frequência. Assim, $\sigma(k\omega_s)$ é o valor de $\sigma(\omega)$ em $\omega = k\omega_s$ sendo k número inteiro. Como pode ser observado em (4.5), o estado contínuo de um fóton é aproximado por uma superposição do produto tensorial de osciladores discretos sendo que cada oscilador trabalha em uma única frequência. Por exemplo, o estado $\left|\tilde{1}\right\rangle_k = |0\rangle_1 \ldots |1\rangle_k \ldots |0\rangle_N$ significa um fóton na frequência $k\omega_s$ e zero fóton nas outras frequências. O número de osciladores discretos N é igual ao número de amostras de $\sigma(\omega)$ e a amplitude de probabilidade do k-ésimo termo na superposição é dada por $\sigma(k\omega_s)(\omega_s)^{1/2}$. Para estados de dois fótons entrelaçados em (4.7) tem-se que com probabilidade $|\sigma(k\omega_s, l\omega_s)|^2 \omega_s$ os fótons nas frequências $k\omega_s$ e $l\omega_s$ ($k\omega_s + l\omega_s = M\omega_s = 2\omega_0$) estão no estado entrelaçado $(|HH\rangle + |VV\rangle)/2^{1/2}$. Por fim, (4.9) mostra que o estado coerente contínuo pode ser aproximado por um produto tensorial de estados coerentes de uma única frequência tendo amplitude $\alpha(k\omega_s)(\omega_s)^{1/2}$ na frequência $\omega = k\omega_s$.

5 COMUNICAÇÃO QUÂNTICA SEGURA DIRETA DE SINAIS ANALÓGICOS E DIGITAIS USANDO ESTADOS COERENTES

5.1 Introdução

A distribuição de chave quântica é um protocolo quântico bem estudado (NAMEKATA, 2007; LO; ZHAO, 2012) que alcançou o estágio comercial. Uma propriedade intrínseca dos protocolos de QKD é o fato de que a chave final é uma sequência aleatória de bits não controlado por nenhum dos participantes legítimos, Alice e Bob. Isso ocorre porque, nas regras dos protocolos de QKD, pelo menos um deles faz modulações aleatórias no sinal óptico ou escolha aleatória da base de medição. Uma alternativa é a QSDC (CHANG *et al*., 2013; DENG *et al*., 2003; LIU, *et al*., 2013; LONG; LIU, 2002). Em tais protocolos, a comunicação é determinística, no sentido de que, na ausência de ruído, o emissor controla a informação recebida pelo receptor. Assim, a QSDC é útil para a transmissão segura de qualquer tipo de mensagem, incluindo uma chave criptográfica.

Na literatura sobre QSDC, com exceção do protocolo proposto por (MENDONÇA; DE BRITO; RAMOS, 2012), todos os outros protocolos de QSDC encontrados na literatura (até o momento atual) requerem pelo menos um recurso quântico que não está disponível com a tecnologia de hoje. Nesta direção, a presente seção descreve configurações ópticas utilizando apenas dispositivos ópticos lineares comuns, detectores de fótons únicos baseados em fotodiodos de avalanche (APD) e fontes de luz coerentes e térmicas, para executar o protocolo QSDC de sinais digitais e analógicos.

Um ponto crucial na segurança dos esquemas aqui propostos é a largura espectral de estados coerentes contínuos. Usando uma modulação de fase dependente da frequência, Alice pode esconder a modulação de fase aplicada por Bob, tornando os esquemas propostos altamente seguros. Por fim, o esquema para QSDC de sinais analógicos utiliza na detecção um receptor óptico baseado em fotodiodo PIN, o que torna a sua implementação mais fácil e mais barata.

Este capítulo está estruturado na seguinte forma: Na Seção 5.2, os estados coerentes contínuos são revisados e sua interferência quântica é descrita. Na Seção 5.3 são

apresentadas as configurações ópticas para QSDC de sinais digitais. Na Seção 5.4 é apresentada a configuração óptica para QSDC de sinais analógicos.

5.2 Estados Coerentes Contínuos

Uma breve revisão sobre estado contínuos da luz está descrito na seção 4. Aqui é descrito apenas o estado coerente contínuo. Ele é definido de acordo como Santos *et al*. (1997).

$$\left|\alpha_{\omega}\right\rangle = \exp\left[\int\left[\alpha(\omega)a^{\dagger}(\omega)-\alpha^{*}(\omega)a(\omega)\right]d\omega\right]\left|0_{\omega}\right\rangle, \tag{5.1}$$

$$\langle n\rangle = \int_{0}^{\infty}\left|\alpha(\omega)\right|^{2} d\omega. \tag{5.2}$$

Em (5.2) $\langle n\rangle$ é o número médio de fótons do estado $|\alpha_{\omega}\rangle$ e $\alpha(\omega)$ é a amplitude complexa do campo. Agora, pode-se escrever $\alpha(\omega)$ na base de funções sinc:

$$\alpha(\omega) = \sum_{k=-\infty}^{\infty}\alpha(k\omega_{S})\,\mathrm{sinc}\left[(\omega-k\omega_{S})/\omega_{S}\right], \tag{5.3}$$

$$\mathrm{sinc}(x) = \sin(\pi x)/\pi x. \tag{5.4}$$

Em (5.3) ω_S é o tamanho do passo de discretização no domínio da frequência. Usando a ortogonalidade da função sinc,

$$\frac{1}{\omega_{s}}\int_{-\infty}^{\infty}\mathrm{sinc}\left[\frac{(\omega-k\omega_{s})}{\omega_{s}}\right]\mathrm{sinc}\left[\frac{(\omega-m\omega_{s})}{\omega_{s}}\right]d\omega = \delta_{km}. \tag{5.5}$$

e o fato de $\alpha(\omega)$ ser zero pra frequências negativas, tem-se que,

$$\langle n\rangle = \int_0^{\infty} \left|\alpha(\omega)\right|^2 d\omega = \int_{-\infty}^{\infty} \left|\alpha(\omega)\right|^2 d\omega = \sum_{k=1}^{\infty} \left|\alpha(k\omega_s)\right|^2 \omega_s . \tag{5.6}$$

Conforme Ramos e Souza (2001) a equação (5.6) mostra como deixar discreto o estado coerente contínuo, ou seja, o estado coerente contínuo pode ser aproximado por um produto tensorial de estados coerentes com uma única frequência. Se $\alpha(\omega)$ se anula para $\omega > N\omega s$, então apenas um número finito de modos é necessário e, portanto,

$$\left|\alpha_{\omega}\right\rangle = \prod_{k=1}^{N} \left|\alpha(k\omega_S)\sqrt{\omega_S}\right\rangle . \tag{5.7}$$

Como pode ser observado em (5.7), o número de osciladores discretos é igual ao número de amostras tomadas a partir da envoltória do campo. Cada oscilador discreto está num estado coerente e a amplitude do *k*-ésimo oscilador é igual ao produto da *k*-ésima amostra de $\alpha(\omega)$ pela da raiz quadrada de ω_s.

Considere-se, agora, um interferômetro de *Mach-Zenhder* (MZI) em que os moduladores de fase são dependentes da frequência. Em outras palavras, cada componente espectral do campo recebe um deslocamento de fase diferente. O MZI é composto por dois divisores de feixe sem perdas com a transmitância $T = 1/2^{1/2}$ (e refletância $R = i\,1/2^{1/2}$, e um modulador de fase em cada braço, $\phi_A(\omega)$ e $\phi_B(\omega)$. Tendo como entrada no MZI o estado $|\alpha_{\omega}\rangle|0_{\omega}\rangle$, o estado total na saída é:

$$\left|\psi(\omega)\right\rangle = \prod_{k=1}^{N} \left|\alpha(k\omega_S)\sqrt{\omega_S}e^{i\Omega_k}\cos(\Delta_k)\right\rangle \left|\alpha(k\omega_S)\sqrt{\omega_S}e^{i\Omega_k}\sin(\Delta_k)\right\rangle \tag{5.8}$$

$$\Omega_k = \left[\phi_A(k\omega_S) + \phi_B(k\omega_S)\right]/2;\ \Delta_k = \left[\phi_A(k\omega_S) - \phi_B(k\omega_S)\right]/2. \tag{5.9}$$

Assim, os números médios de fótons na saída do interferômetro são:

$$\langle n_1 \rangle = \sum_{k=1}^{N} \left|\alpha\left(k\omega_S\right)\right|^2 \cos^2\left(\frac{\phi_A\left(k\omega_S\right)-\phi_B\left(k\omega_S\right)}{2}\right)\omega_S, \tag{5.10}$$

$$\langle n_2 \rangle = \sum_{k=1}^{N} \left|\alpha\left(k\omega_S\right)\right|^2 \sin^2\left(\frac{\phi_A\left(k\omega_S\right)-\phi_B\left(k\omega_S\right)}{2}\right)\omega_S, \tag{5.11}$$

ou, retornando para o caso contínuo,

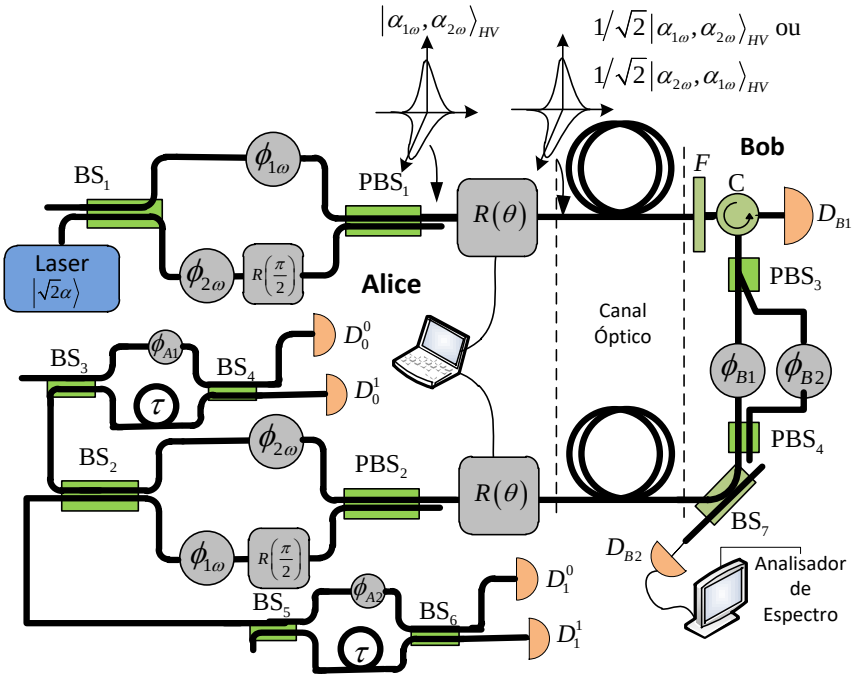
$$\langle n_1 \rangle = \int_0^{\infty} \cos^2\left[\frac{\phi_A(\omega)-\phi_B(\omega)}{2}\right]\left|\alpha\left(\omega\right)\right|^2 d\omega, \tag{5.12}$$

$$\langle n_2 \rangle = \int_0^{\infty} \sin^2\left[\frac{\phi_A(\omega)-\phi_B(\omega)}{2}\right]\left|\alpha\left(\omega\right)\right|^2 d\omega. \tag{5.13}$$

5.3 Comunicação Quântica Segura Direta de Sinal Digital

O objetivo de usar estados contínuos em protocolos de QSDC é de aumentar a segurança. O primeiro esquema óptico para QSDC usando estados coerentes contínuos e moduladores de fase dependente da frequência é mostrado na FIGURA 6.

Figura 6 – Configuração Óptica I para QSDC de sinais digitais usando estados coerentes contínuos.



Fonte: Guerra *et al*. (2016).

O esquema da FIGURA 6 funciona da seguinte forma: inicialmente, usando o divisor de feixes (*beam splitter*) BS_1, os elementos dispersivos $\phi_{1\omega}$ e $\phi_{2\omega}$ ($\phi_{1\omega}$ e $\phi_{2\omega}$ introduzem uma modulação de fase diferente em cada componente espectral do sinal óptico), o rotacionador de polarização de $\pi/2$ e o divisor de feixe por polarização (*polarization beam splitter*) PBS_1, Alice produz um estado de dois modos $|\alpha_{1\omega},\ \alpha_{2\omega}\rangle_{HV}$ (H e V representam modos de polarização horizontal e vertical). Em seguida, usando $R(\theta)$ Alice gira aleatoriamente a sua polarização por 0 ou $\pi/2$. Assim, o estado quântico lançado no canal óptico é:

$$\rho_A = 0{,}5\left|\alpha_{1\omega},\alpha_{2\omega}\right\rangle_{HV}\left\langle\alpha_{1\omega},\alpha_{2\omega}\right| + 0{,}5\left|\alpha_{2\omega},\alpha_{1\omega}\right\rangle_{HV}\left\langle\alpha_{2\omega},\alpha_{1\omega}\right|. \tag{5.14}$$

Quando este estado passa por Bob, cada modo de polarização é modulado em fase. Assim, o estado quântico partindo de Bob é:

$$\rho_B = 0{,}5\left|\alpha_{1\omega}e^{i\phi_{B1}},\ \alpha_{2\omega}e^{i\phi_{B2}}\right\rangle_{HV}\left\langle\alpha_{1\omega}e^{i\phi_{B1}},\ \alpha_{2\omega}e^{i\phi_{B2}}\right| + 0{,}5\left|\alpha_{2\omega}e^{i\phi_{B1}},\ \alpha_{1\omega}e^{i\phi_{B2}}\right\rangle_{HV}\left\langle\alpha_{2\omega}e^{i\phi_{B1}},\ \alpha_{1\omega}e^{i\phi_{B2}}\right| \tag{5.15}$$

Bob escolhe aleatoriamente um dos valores $\{0,\ \pi,\ \pi/2,\ 3\pi/2\}$ para ϕ_{B1} e ϕ_{B2}, no entanto, se ele quer transmitir o bit 0 (1), ele faz $\phi_{B1} - \phi_{B2} = 0\ (\pi)$. O estado em (5.15) é enviado de volta para Alice. Alice, por sua vez, aplica uma rotação de polarização de 0 ou $\pi/2$, de tal forma que, o pulso que passou através do elemento dispersivo $\phi_{1\omega}(\phi_{2\omega})$ na transmissão, passará agora pelo elemento dispersivo $\phi_{2\omega}(\phi_{1\omega})$. Adicionalmente, uma rotação de polarização de $\pi/2$ é aplicada em um dos pulsos. Desta forma, os dois pulsos chegarão ao BS_2 ao mesmo tempo, com a mesma polarização e diferença de fase igual a $\phi_{B1} - \phi_{B2}$. Se $\phi_{B1} - \phi_{B2} = 0$, a luz é enviada para o interferômetro superior composto por $BS_3 - \phi_{A1} - BS_4$ e detectada em D_0^0 ou D_0^1, o que implica a detecção de um bit '0'. Por outro lado, se $\phi_{B1} - \phi_{B2} = \pi$, a luz é enviada para o interferômetro inferior composto por $BS_5 - \phi_{A2} - BS_6$ e detectada em D_1^0 ou D_1^1, o que implica a detecção de um bit '1'. Alice escolhe aleatoriamente um dos valores $\{0,\ \pi/2\}$ para ϕ_{A1} e ϕ_{A2}. A segurança deste esquema baseia-se em duas condições:

1) Os segredos conhecidos apenas por Alice: o número médio de fótons do estado coerente contínuo usado, as funções $\phi_{1\omega}$ e $\phi_{2\omega}$ e quais estados estão nas polarizações horizontal e vertical;

2) A distribuição diferencial em quadratura de chaves que funciona em paralelo. Para a espiã, Eve, obter qualquer informação sobre as modulações de Bob, ela pode tentar fazer interferência entre os pulsos ópticos provenientes de Bob, no entanto, sem saber $\phi_{1\omega}$ e $\phi_{2\omega}$, ela não será capaz de obter qualquer informação útil uma vez que ela estará limitada por (5.12) e (5.13).

Em outras palavras, usando um divisor de feixe para fazer a interferência dos pulsos provenientes de Bob (primeiro Eve tem que girar de $\pi/2$ a polarização de um deles), Eve obterá os seguintes números médios de fótons em suas saídas do divisor de feixe:

$$\langle n_1 \rangle = \int_0^\infty \cos^2\left[\frac{(\phi_{1\omega}(\omega) - \phi_{2\omega}(\omega)) + (\phi_{B1} - \phi_{B2})}{2}\right] |\alpha(\omega)|^2\, d\omega, \tag{5.16}$$

$$\langle n_2 \rangle = \int_0^\infty \sin^2\left[\frac{(\phi_{1\omega}(\omega) - \phi_{2\omega}(\omega)) + (\phi_{B1} - \phi_{B2})}{2}\right] |\alpha(\omega)|^2\, d\omega. \tag{5.17}$$

Portanto, os números médios de fótons nas saídas dependem de $\phi_{1\omega}$ e $\phi_{2\omega}$, que não são conhecidos por Eve. O pior caso para Eve ocorre quando $\phi_{1\omega}$ e $\phi_{2\omega}$ são escolhidos de tal forma que,

$$\int_0^{\infty} \cos\left[\phi_{1\omega}(\omega)-\phi_{2\omega}(\omega)\right]\left|\alpha(\omega)\right|^2 d\omega = 0, \tag{5.18}$$

pois neste caso $\langle n_1\rangle = \langle n_2\rangle$. Eve pode ainda tentar descobrir os valores das funções $\phi_{1\omega}$ e $\phi_{2\omega}$. Para evitar este ataque, o número médio de fótons dos pulsos deve ser baixo o suficiente. Se $\phi_{1\omega}$ e $\phi_{2\omega}$ são funções com baixa autocorrelação (ou seja, são quase-aleatórias), um número médio de fótons igual a 0,1 fótons por frequência seria uma boa escolha, já que Eve teria que descobrir o valor de cada frequência independentemente. No entanto, na prática, as funções $\phi_{1\omega}$ e $\phi_{2\omega}$ produzidas por um elemento óptico dispersivo tendem a ser suaves e bem comportadas. Neste caso, uma escolha mais conservadora de menos de um fóton por pulso (isto é, considerando todas as frequências) em média tornaria o sistema mais seguro. No caso extremo de $\phi_{1\omega}$ e $\phi_{2\omega}$ serem constantes (independente da frequência), o caso tradicional de 0,1 fótons por pulso é recuperado.

Outra possibilidade para Eve obter informações sobre as modulações de Bob é ela mesma enviar pulsos ópticos para Bob e analisá-los após as modulações de Bob. Para evitar esse ataque, Bob usa três contramedidas:

1) Ele tem um filtro *F* que força Eve a usar o comprimento de onda que os detectores de Bob "enxergam";

2) Ele usa o circulador *C* e o detector D_{B1} para fazer sua configuração unidirecional. Ou seja, Eve tem que atacar pela fibra que vêm de Alice e não pela que sai de Bob;

3) Ele usa um detector de fótons, D_{B2}, conectado a um analisador de espectro elétrico (*Electrical Spectrum Analyzer* – ESA) e verifica a potência elétrica em uma banda de frequência fixa. Esta potência elétrica dependerá da distribuição do número de fótons do estado de luz quântica incidente e, portanto, do número médio de fótons usado por Alice (CAVALCANTI *et al*., 2011; KAWAKAMI *et al*., 2015; MENDONÇA *et al*., 2012).

Assim, se Eva não conhecer o valor correto do número médio de fótons ou enviar pulsos fora dos intervalos de tempo corretos, sua interferência resultará num valor diferente para a potência elétrica medida. No final da comunicação, Bob informa à Alice a potência elétrica medida e Alice verifica se esse valor está de acordo com o número médio de fótons usado por ela. Isso evita, por exemplo, o uso de pulsos ópticos fortes que poderia facilitar a tarefa de Eve na obtenção dos valores de $\phi_{1\omega}$ e $\phi_{2\omega}$. De um ponto de vista prático, Alice aceitará um valor medido por Bob dentro de um intervalo em torno do valor esperado. Neste caso, Eve não precisa saber o valor exato do número médio de fótons usado por Alice; uma boa aproximação pode ser suficiente. Neste sentido vamos considerar a seguinte situação: Eve quebra o enlace óptico entre Alice e Bob. Ela usa um divisor de feixe (com valor de reflexividade igual à perda na fibra entre Alice e Bob) na saída de Alice. Em uma saída, Eve usa a mesma configuração de medição que Bob (um único detector de fótons conectado a um analisador espectral) para obter uma estimativa α_{est} do número médio de fótons usado por Alice. Depois disso, ela prepara e envia a Bob o estado quântico $|\alpha_{est},\ \alpha_{est}\rangle_{HV}$.

Na saída de Bob, Eve obtém o estado $\left|\alpha_{est}e^{i\phi_{B1}},\ \alpha_{est}e^{i\phi_{B2}}\right\rangle_{HV}$. Como $\phi_{B1}-\phi_{B2}=0$ ou π (os casos em que $\phi_{B1}-\phi_{B2}$ é igual a $\pi/2$ ou $3\pi/2$ são discutidos posteriormente), Eve pode usar um divisor de feixe simples para fazer sua interferência e obter o valor do bit enviado por Bob. Agora, de acordo com esse resultado, Eve modula a parte não detectada (estava armazenada em uma memória óptica) do pulso enviado por Alice e a envia de volta para Alice por uma fibra sem perdas. Há dois problemas neste ataque. Em primeiro lugar, Eve vai precisar de muitos pulsos enviados por Alice, a fim de obter uma boa estimativa do número médio de fótons utilizado (CAVALCANTI *et al*., 2011). Enquanto ela ainda está medindo, ela terá que enviar pulsos para Bob com um número de fóton médio adivinhado (a falta de luz que chega em Bob resultará em uma potência elétrica igual ao ruído de fundo). Em segundo lugar, como pode ser observado na FIGURA 6, existe uma distribuição quântica de chave com deslocamento diferencial de fase em quadratura (*Differential Quadrature Phase-Shift Quantum Key Distribution*, DQPS-QKD) funcionando em paralelo.

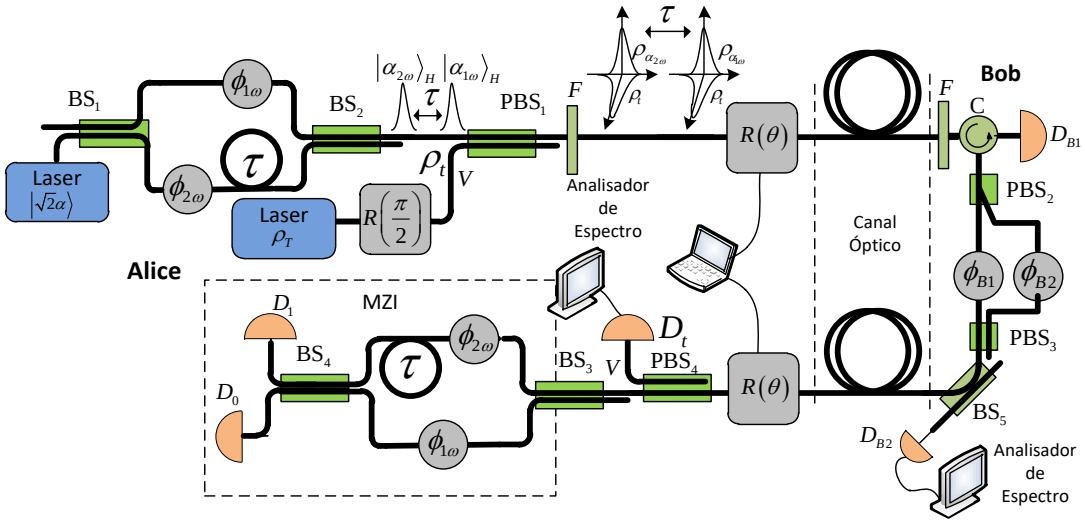
Mesmo quando Eve pode determinar o bit do protocolo QSDC enviado por Bob $(\phi_{B1}-\phi_{B2})$, ela não pode determinar os valores de ϕ_{B1} e ϕ_{B2} separadamente e, portanto, ela irá introduzir erros no protocolo de QKD, o que será observado por Alice após a comunicação clássica entre Bob e ela. Deve-se notar que as situações em que $\phi_{B1}-\phi_{B2}$ é igual a $\pi/2$ ou

$3\pi/2$ são estados isca. No final do protocolo, Bob informa a Alice em quais slots de tempo ele usou um estado isca, e o bit correspondente é descartado.

A configuração óptica do protocolo DQPS-QKD incorporada na configuração óptica do protocolo QSDC é composta por ϕ_{B1} e ϕ_{B2} em Bob e os interferômetros superiores $BS_3 - \phi_{A1} - BS_4$ e inferiores $BS_5 - \phi_{A2} - BS_6$ em Alice. Suas regras e segurança estão bem descritas segundo (INOUE; IWAI, 2009; KAWAKAMI *et al*., 2016). A taxa de erro na chave obtida neste protocolo de QKD é usada para inferir a presença de Eve, embora outras aplicações para esta chave também possam ser realizadas. Por fim, deve-se notar que após a interferência em BS_2 a fase do pulso de saída é $\phi_{B1} + \phi_{B2}$. Portanto, a diferença de fase entre dois pulsos consecutivos, *n*-ésimo e (n+1)-ésimo, no protocolo de QKD é $[\phi_{B1}(n) + \phi_{B2}(n)] - [\phi_{B1}(n+1) + \phi_{B2}(n+1)]$. Dependendo do valor de $\phi_{B1}(n) - \phi_{B2}(n)$ e $\phi_{B1}(n+1) - \phi_{B2}(n+1)$ a configuração de QKD usa $BS_3 - \phi_{A1} - BS_4$ ou $BS_5 - \phi_{A2} - BS_6$.

A segunda configuração para QSDC de mensagens digitais é mostrada na FIGURA 7. Comparando com a primeira configuração mostrada na FIGURA 6, tem a segurança melhorada pelo uso de estados térmicos. Uma discussão detalhada sobre a segurança dos protocolos quânticos de duas camadas usando estados coerentes e térmicos pode ser encontrada em (PINHEIRO; RAMOS, 2015).

Figura 7 – Esquema óptico II para QSDC de mensagens digitais



Fonte: Guerra *et al*. (2016).

A configuração óptica na FIGURA 7 funciona da seguinte maneira: Alice produz dois pulsos ópticos, separados no tempo por τ. O primeiro pulso está no estado $(\rho_1 \otimes \rho_T)_{HV}$ enquanto o segundo está no estado $(\rho_2 \otimes \rho_T)_{HV}$ sendo $\rho_1 = |\alpha_{1\omega}\rangle\langle\alpha_{1\omega}|$, $\rho_2 = |\alpha_{2\omega}\rangle\langle\alpha_{2\omega}|$ e ρ_T é a matriz de densidade do estado térmico, $\rho_T = \sum_n \left[\mu_T^n / \left(1+\mu_T{}^{1+n}\right)\right] |n\rangle\langle n|$, nesta, μ_T é o número médio de fótons. Após o primeiro rotacionador de polarização $R(\theta)$ de Alice, o primeiro pulso lançado no canal é $1/2\,(\rho_1 \otimes \rho_T)_{HV} + 1/2\,(\rho_T \otimes \rho_1)_{HV}$ enquanto o segundo pulso está no estado $1/2\,(\rho_2 \otimes \rho_T)_{HV} + 1/2\,(\rho_T \otimes \rho_2)_{HV}$. No entanto, Alice age de tal forma que, se ρ_1 está no modo horizontal (vertical) ρ_2 estará no modo vertical (horizontal). Quando os pulsos chegam a Bob, eles são modulados em fase (pode-se observar que os estados térmicos não são afetados pela modulação de fase de Bob) e enviados de volta para Alice. Alice, por sua vez, aplica uma rotação na polarização de tal maneira que o estado térmico sempre emerge na saída vertical de PBS_4. Por outro lado, os pulsos horizontais são enviados para um interferômetro com um atraso de τ em um dos braços. Em sua saída haverá interferência entre os pulsos que tomaram os caminhos curto-longo e longo-curto nos interferômetros de Alice. A diferença de fase entre os pulsos que sofrerão interferência é igual a $\phi_{B1} - \phi_{B2}$. Mais uma vez, se $\phi_{B1} - \phi_{B2} = 0\ (\pi)$, uma detecção ocorre em $D_0\ (D_1)$ e um bit $0\ (1)$ é registrado.

Novamente, a segurança deste esquema baseia-se nos segredos conhecidos apenas por Alice: o número médio de fótons usado para os estados térmico e coerente, as funções de $\phi_{1\omega}$ e $\phi_{2\omega}$ e quais estados estão nas polarizações horizontais e verticais. Para que Eve obtenha qualquer informação sobre a modulação de Bob, ela tem que fazer interferência entre os pulsos ópticos provenientes de Bob, no entanto, ela não sabe em qual modo de polarização os estados coerentes estão e quais são as funções $\phi_{1\omega}$ e $\phi_{2\omega}$, portanto, ela não será capaz de obter qualquer informação útil.

Como aconteceu no primeiro esquema, outra possibilidade para Eve é enviar pulsos ópticos para Bob e analisá-los após as modulações de Bob. Como antes, Bob usa o filtro *F*, o circulador *C* juntamente com o detector D_{B1} e um detector de fótons únicos, o D_{B2}, conectado a um ESA. A potência elétrica medida pelo ESA dependerá dos números médios de fótons escolhidos por Alice para os estados térmico e coerente. Sem saber o valor exato daqueles números médios de fótons ou enviar pulsos fora dos intervalos de tempo corretos, resultará num valor diferente para a potência elétrica medida. No final da comunicação, Bob

informa à Alice a potência elétrica medida e Alice verifica se esse valor está de acordo com os números médios de fótons usados.

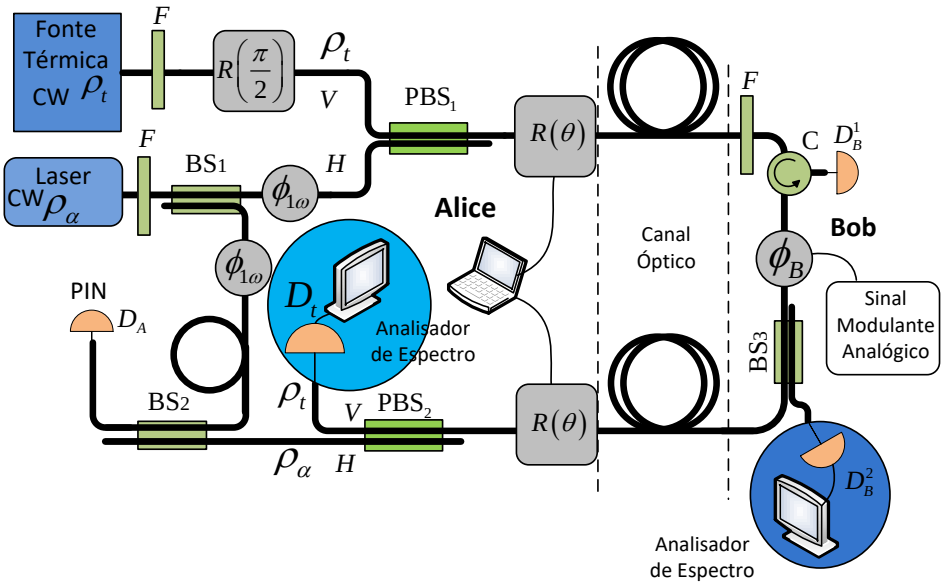
Como Alice usa pulsos com número médio de fótons baixo, às vezes, ela não terá qualquer detecção em D_0 e D_1. Nesses casos, Alice informa a Bob os intervalos de tempo em que ela não teve qualquer detecção, e eles executam o protocolo novamente até que a informação completa seja transmitida de Bob para Alice. Embora não esteja mostrado na FIGURA 7, o protocolo DQPS-QKD pode ser facilmente incluído nesta configuração colocando os interferômetros superiores e inferiores da FIGURA 6 em Alice.

5.4 Comunicação Quântica Segura Direta de Sinais Analógicos

Os detectores de fótons únicos baseados em APDs são caros e têm que ser resfriados para diminuir a corrente de escuro, que pode sinalizar uma foto-detecção falsa. Os APDs têm problemas para operar em altas taxas de transmissão devido ao *afterpulsing* e eles têm baixa eficiência quântica na janela óptica de 1.550 nm. Portanto, configurações ópticas para comunicação quântica usando receptores ópticos baseados em PIN são altamente desejadas, uma vez que os fotodiodos PIN são mais baratos, mais rápidos e não precisam ser resfriados.

Encontra-se na literatura esquemas de QKD utilizando receptores ópticos baseados em PIN. No entanto, todos estes protocolos baseiam-se nas medições das quadraturas do campo e, portanto, utilizam dois detectores PIN. Na direção oposta, o esquema óptico para QSDC de dados analógicos aqui proposto utiliza apenas um detector PIN, como mostrado na FIGURA 8. Uma vez que a informação a ser transmitida é um sinal analógico, as fontes de luz são CW.

Figura 8 – Esquema óptico III para QSDC de mensagens analógicas.



Fonte: Guerra *et al*. (2016).

O protocolo de QSDC de sinal analógico pode ser entendido da seguinte forma: o estado coerente emitido pela fonte coerente CW de Alice é dividido pelo divisor de feixe BS_1 não balanceado em dois campos: sinal (ρ_{sinal} - com número médio de fótons menor que 1) e oscilador local (ρ_{LO} - com número médio de fótons alto). Os estados de sinal e oscilador local passam através dos mesmos dispositivos ópticos dispersivos e obtêm a modulação de fase dependente da frequência. Além disso, ρ_{LO} é atrasado para compensar o tempo necessário para o pulso enviado a Bob, ρ_{sinal}, retornar ao dispositivo de Alice. Uma vez em Bob, os feixes de luz são modulados em fase por um sinal analógico.

Mais uma vez, o estado térmico não é afetado pelo modulador de fase de Bob. Na entrada do dispositivo de Alice, deve ser aplicada a mesma rotação de polarização para assegurar o estado térmico na polarização vertical e o sinal (estado coerente) na polarização horizontal. O primeiro é enviado para o analisador de estado (detector de fótons únicos e ESA), enquanto o segundo é enviado diretamente para um receptor óptico baseado em PIN. Como aconteceu nos outros esquemas propostos, a segurança baseia-se nos segredos conhecidos apenas por Alice: os números médios de fótons dos estados coerentes e térmicos, a codificação da polarização e o valor de $\phi_{1\omega}$. Sem saber $\phi_{1\omega}$ e onde está o estado coerente, Eve não pode obter qualquer informação útil. O sinal analógico de Bob aparece na fotocorrente do PIN, como será mostrado na seção 3.

6 DETECÇÃO HOMÓDINA DE FÓTONS ÚNICOS

6.1 Introdução

Os sistemas de transmissão por fibras ópticas em geral empregam a modulação direta da intensidade do sinal óptico, normalmente gerado por lasers semicondutores, e a detecção direta através de fotodiodos PIN ou avalanche. A variação da potência da luz se transforma em variação de corrente que flui pelo fotodiodo. Entretanto, a partir de 1980, verificou-se um esforço crescente na pesquisa de sistemas de comunicação óptica que carregam a informação na fase. Estes sistemas são chamados de sistemas coerentes.

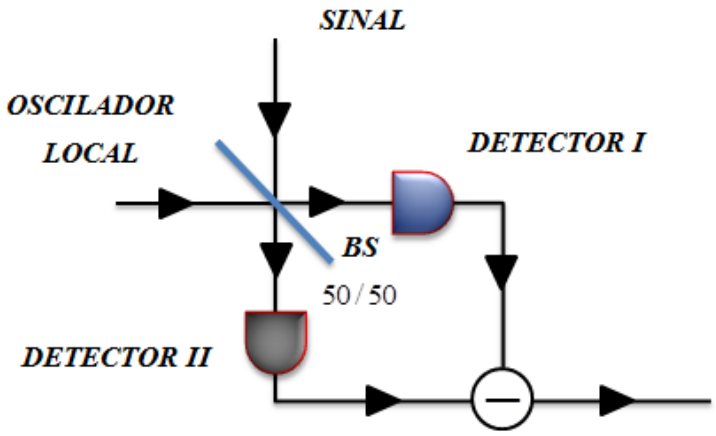
A detecção da luz em sistemas coerentes utiliza outro feixe de luz, usado como referência, usualmente chamado de oscilador local. Quando o oscilador local possui a mesma frequência do sinal a ser medido, o método de detecção é denominado detecção homódina. Caso contrário tem-se a detecção heteródina (LEONHARDT, 1997). Este tipo de medição foi utilizado na seção anterior o qual trata-se dos protocolos de QSDC.

De acordo com Silva *et al*. (2006) para obter taxas de chave em QKD substancialmente mais elevadas, a detecção homódina constitui uma alternativa interessante para a contagem de fótons, porque quando usada com um oscilador local de potência adequada para operação perto do limite de ruído quântico, fornece o ganho de mistura para superar o ruído térmico, empregando convencionalmente o fotodiodo PIN que funciona à temperatura ambiente, que apresentam uma eficiência quântica e uma velocidade de resposta muito superior em comparação com APD, além de menor custo e requisitos mais simples.

6.2 Detecção Heteródina Óptica

O diagrama esquemático da detecção heteródina é mostrado na FIGURA 9.

Figura 9 – Diagrama da detecção Heteródina (Homódina). Combinação do sinal de informação com o sinal do oscilador local.



Fonte: adaptada de Haus (2000).

O sinal óptico recebido e o sinal laser local são combinado em um divisor de feixes balanceado. O *BS* reflete metade da potência incidente e transmite a outra metade. Um fotodetector é colocado em cada saída do *BS*. A fotocorrente é dada por:

$$\mathcal{R}_0 = \frac{q\eta}{hf} \quad (A/W), \tag{6.1}$$

$$i_{ph} = \mathcal{R}_0 P_i = \mathcal{R}_e \left\langle e_i^2 \right\rangle. \tag{6.2}$$

A responsividade do fotodiodo, $\mathcal{R}_0$, depende das propriedades intrínsecas do fotodiodo e varia com o comprimento de onda. A unidade é Ampere por Watt. Além disso, η é a eficiência quântica, h é a constante de Planck, f é a frequência do sinal óptico, q é a carga do elétron, P_i é a potência óptica incidente e a constante $\mathcal{R}_e$ inclui a responsividade e as constantes necessárias para converter de watts para $(V/m)^2$.

Assumindo que os dois campos na entrada do *BS* têm a mesma polarização, o campo elétrico na entrada é a soma do campo elétrico da portadora modulada, e_1, com o campo elétrico do laser local, e_0; Assim, a fotocorrente fica dada por:

$$i_{ph} = \mathcal{R}_e \left\langle e_i^2 \right\rangle = \mathcal{R}_e \left\langle \left(e_1 + e_0\right)^2 \right\rangle = \mathcal{R}_e \left\langle \left(e_1^2 + 2e_1e_0 + e_0^2\right) \right\rangle, \tag{6.3}$$

sendo e_1 e e_0 dados, respectivamente, por

$$e_1 = E_1\left[1 + mf\left(t\right)\right]\cos\left(\omega_1 t\right) \tag{6.4}$$

$$e_0 = E_0 \cos\left(\omega_0 t\right) \tag{6.5}$$

Pode-se observar que e_1 tem sua amplitude modulada. Substituindo as equações (6.4) e (6.5) em (6.3) encontra-se uma equação para a fotocorrente no fotodiodo, expandindo o produto dos termos do cosseno e negligenciando os termos de alta frequência,

$$i_{ph} = \mathcal{R}_e \left\{ \frac{1}{2} E_1^2 \left[1 + mf\left(t\right)\right]^2 + \frac{1}{2} E_0^2 + E_0 E_1 \left[1 + mf\left(t\right)\right] \cos\left(\omega_1 - \omega_0\right) t \right\}. \tag{6.6}$$

Na detecção heteródina, espera-se que $E_0 >> E_1$, então:

$$i_{ph} = \mathcal{R}_e \left\{ \frac{1}{2} E_0^2 + E_0 E_1 \left[1 + mf\left(t\right)\right] \cos\left(\omega_1 - \omega_0\right) t \right\}. \tag{6.7}$$

A corrente consiste de um termo *dc* e um termo de frequência intermediária (ω_1 - ω_0). Este último pode ser amplificado e recuperado em uma demodulação; o envelope $f(t)$ detectado produz uma voltagem na saída da forma:

$$\mathrm{v} = A\mathcal{R}_e E_0 E_1 mf\left(t\right). \tag{6.8}$$

A constante *A* depende do circuito eletrônico de detecção. Em termos de potência óptica, tem-se:

$$i \sim \mathcal{R}_0 \left[P_0 P_1\right]^{\frac{1}{2}} mf\left(t\right). \tag{6.9}$$

A equação (6.9) indica que a amplitude do sinal no receptor é proporcional à raiz quadrada da potência dos campos ópticos de sinal e oscilador local. Por isso, se o campo do sinal é fraco, o campo do oscilador local deve ser forte.

Para medições homódinas ópticas, ambas as ondas são virtualmente derivadas da mesma fonte laser. A técnica homódina é sensível à fase no sentido de que a potência do sinal heteródino depende da fase relativa do sinal e do oscilador local. Uma modificação útil é a detecção homódina balanceada, na qual dois fotodiodos são usados após um divisor de feixe 50/50, a soma e a diferença das fotocorrentes são obtidas eletronicamente (JONES JÚNIOR, 1988).

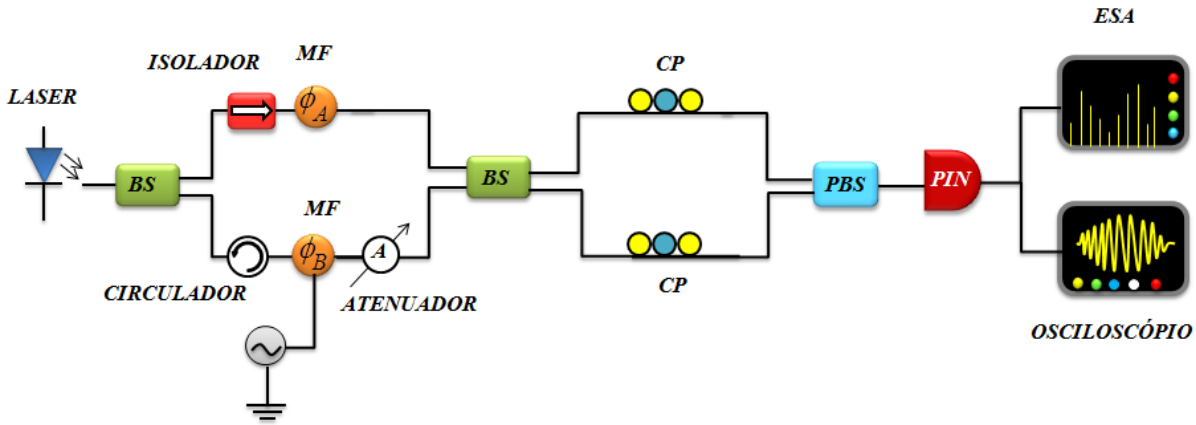
6.3 Construção do Interferômetro de *Mach–Zehnder*

Nesta seção são apresentados os resultados experimentais da construção de um interferômetro de Mach-Zehnder a fibra óptica. Para a construção do Interferômetro foram utilizados os seguintes componentes e equipamentos: laser da THORLABS (Multi Channel Fiber Coupled Laser Source), um gerador de sinais da AGILENT (N9310A RF Signal Generator 9 KHz – 3 GHz), um osciloscópio da ROHDE & SCHWARZ (RTM 1052 Oscilloscope – 500 MHz – 5 GSa/s), um analisador de espectro da ROHDE & SCHWARZ (FSV Signal Analyzer – 10 Hz a 3,6 GHz), dois moduladores de fase da JDS Uniphase, três divisores de feixes (*Beam Spliter* – BS) 50/50, dois circuladores, uma fibra com atenuação de 20 dB, um conector com atenuação de 15 dB e um atenuador variável digital (Digital Variable Attenuator – VOA) de até 60 dB da OZ OPTICS, dois controladores de polarização (CP), e

um divisor de feixe por polarização (*Polarization Beam Splitter* – PBS) e um fotodetector PIN.

Inicialmente montou-se apenas um interferômetro simples, apenas com o laser, dois BS, dois moduladores de fase, mas com o sinal modulante alimentando apenas um dos moduladores de fase, como mostra a FIGURA 10.

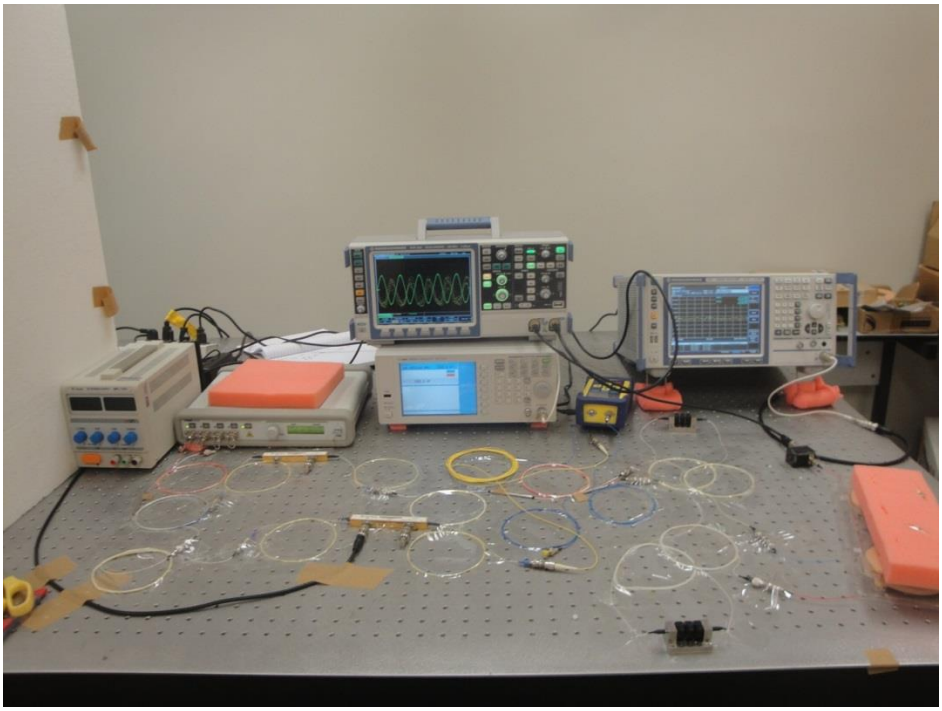
Figura 10 – Interferômetro de *Mach–Zehnder*



Fonte: elaborada pelo autor.

Na FIGURA 11 tem-se uma foto do circuito construído sobre a mesa óptica do Laboratório de Informação Quântica (LATIQ) com os equipamentos em funcionamento. Pode-se observar uma senóide no osciloscópio, que é o sinal detectado pelo PIN resultante da interferência do sinal modulante e o sinal do oscilador local.

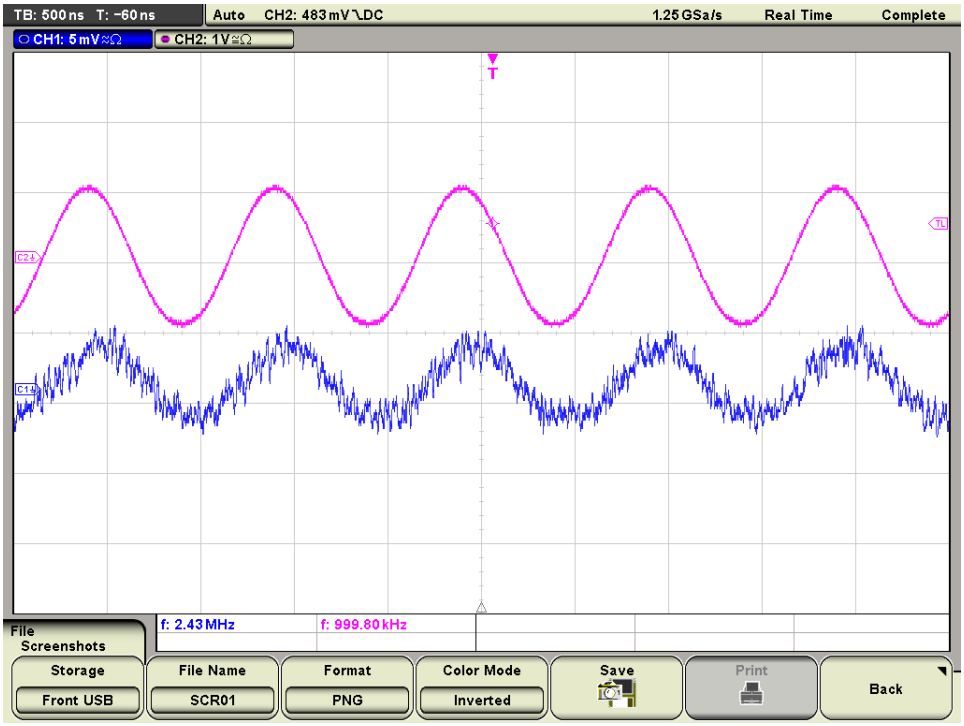
Figura 11 – Circuito montado com Interferômetro de *Mach–Zehnder*.



Fonte: elaborada pelo autor.

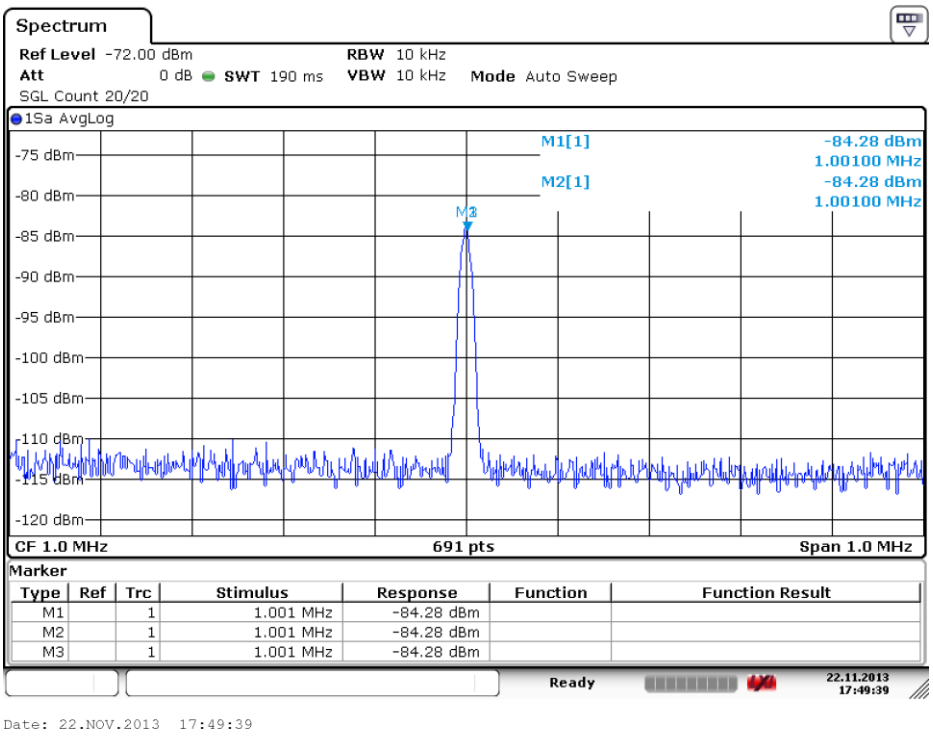
Na FIGURA 12 tem-se a imagem registrada pelo osciloscópio mostrando o sinal modulante e o sinal detectado, enquanto na FIGURA 13 a tela do analisador de espectro é mostrada. A frequência utilizada é de 1 MHz.

Figura 12 – Sinal senoidal visto no osciloscópio.



Fonte: elaborada pelo autor.

Figura 13 – Sinal visto no analisador de espectro com atenuação de 35 dB.



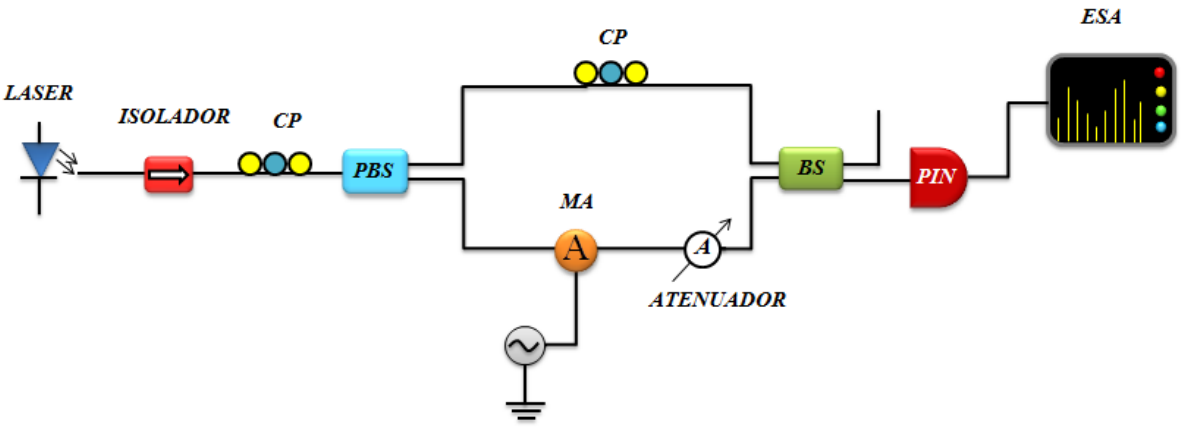
Fonte: elaborada pelo autor.

6.4 Experimento de Detecção de Fótons Únicos com Medição Homódina

O experimento de detecção homódina de fótons únicos consiste em montar um experimento de interferência, sendo que o sinal óptico que carrega a informação na amplitude é fortemente atenuado antes de chegar ao último divisor de feixes onde ocorrerá a interferência. O esquema óptico montado está mostrado nas FIGURAS 14 e 15, diagrama e figura real, respectivamente. O controlador de polarização e o divisor de feixes por polarização na entrada servem como um divisor de feixes com reflexividade ajustável. O diodo laser foi novamente operado bem acima da corrente de limiar, o sinal modulante tinha amplitude de 2.238,8 mV e frequências de 1,0; 1,2; 1,3 e 1,5 GHz.

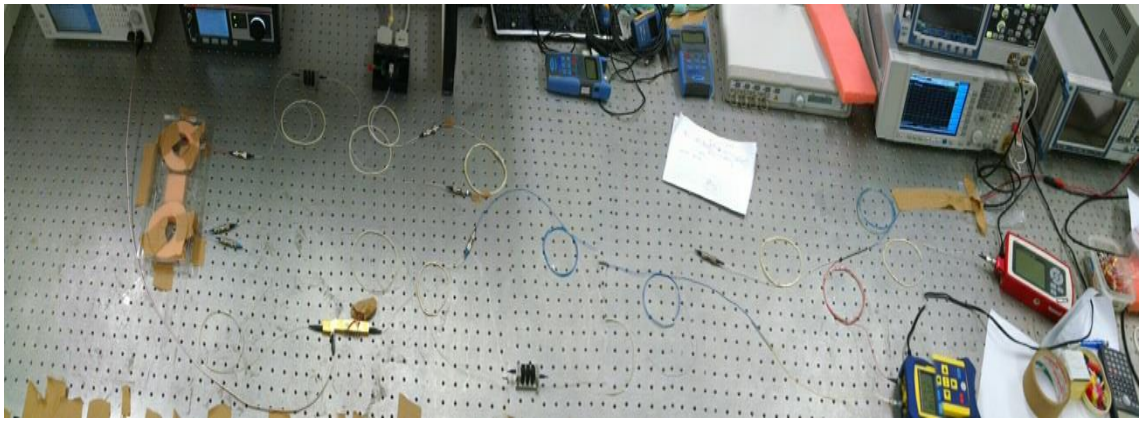
A potência na entrada do PBS é de 5,9±0,3 mW e na saída tem-se aproximadamente em um dos braços 90% do sinal com valor de 5,35 mW (braço do oscilador local) e no outro braço aproximadamente 6% do sinal com valor de 346,9 μW (braço do sinal). A potência média que chega ao BS pelo braço do circuito com 6% da potência total sem atenuação é de 1,642 μW e pelo braço de maior potência é de 4,123 mW.

Figura 14 – Circuito óptico de fótons únicos.



Fonte: elaborada pelo autor.

Figura 15 – Circuito óptico de fótons únicos montado sobre a mesa optica.



Fonte: elaborada pelo autor.

Esta perda de potência deve-se aos moduladores. No braço do sinal há uma atenuação fixa (em fibra) de 20 dB e mais uma atenuação controlada que varia de 1 – 60 dB, portanto, tem-se até 80 dB de atenuação para deixar o sinal no nível de fóton único. Os parâmetros importantes para o cálculo da atenuação requerida são: comprimento de onda λ = 1550 nm, constante de Planck h = 6,626·10^{-34} Js, velocidade da luz c = 3·10^{8} m/s, a potência medida na entrada do divisor de feixes na ausência de atenuação, P_{med} = 1.642 μW e o fluxo médio de fótons desejados n = 0,1. Para o cálculo da atenuação temos as seguintes expressões:

$$nf = \frac{P_{med}10^{-0.1\alpha[dB]}\lambda}{hc} \Rightarrow \alpha = -10\log_{10}\left(\frac{nfhc}{P_{med}\lambda}\right). \qquad (6.10)$$

Sendo que f é a frequência do sinal modulante e α é a atenuação desejada.

Na TABELA 4, têm-se os valores de frequência e de atenuação necessária para que se tenha 0,1 fótons com dois valores diferentes de potência na entrada do BS. As potências utilizadas foram 1,642 μW e 1,542 μW.

Tabela 4 – Atenuação necessária para um regime de 0,1 fótons.

FREQUÊNCIA (GHz)	1,642 µW	1,542 µW
	ATENUAÇÃO α (dB)	
1	51,0733	50,8004
1,2	50,2815	50,0086
1,3	49,9339	49,6610
1,5	49,3124	49,0395

Fonte: elaborada pelo autor.

6.5 Resultados das Medições

Os resultados das medições são apresentados na Tabela 5.

Tabela 5 – Resultados das medições.

FREQUÊNCIA		1.0 GHz			1.2 GHz		
LD	dB	dBm	NÚMERO DE FÓTONS		dBm	NÚMERO DE FÓTONS	
			1,642 µW	1,542 µW		1,642 µW	1,542 µW
ON	21	-95.030	101.7026	95.5088	-94.471	84.7522	79.5907
ON	25	-99.027	40.4885	38.0227	-98.560	33.7405	31.6856
ON	30	-102.608	12.8036	12.0238	-104.117	10.6697	10.0199
ON	35	-107.529	4.0489	3.8023	-108.378	3.3740	3.1686
ON	40	-111.626	1.2804	1.2024	-113.115	1.0670	1.0020
ON	45	-116.263	0.4049	0.3802	-116.690	0.3374	0.3169
ON	46	-116.977	0.3216	0.3020	-117.032	0.2680	0.2517
ON	47	-118.427	0.2555	0.2399	-118.049	0.2129	0.1999
ON	48	-118.818	0.2029	0.1906	-119.272	0.1691	0.1588
ON	49	-119.636	0.1612	0.1514	-120.190	0.1343	0.1261
ON	50	-119.985	0.1280	0.1202	-120.627	0.1067	0.1002
ON	51	-120.637	0.1017	0.0955	-120.918	0.0848	0.0796
ON	52	-120.892	0.0808	0.0759	-121.177	0.0673	0.0632
ON	53	-121.015	0.0642	0.0603	-121.626	0.0535	0.0502
ON	54	-121.694	0.0510	0.0479	-122.334	0.0425	0.0399
ON	55	-122.255	0.0405	0.0380	-122.549	0.0337	0.0317
ON	60	-122.826	0.0128	0.0120	-123.435	0.0107	0.0100
OFF	X	-123.530	0	0	-123.317	0	0
FREQUÊNCIA		1.3 GHz			1.5 GHz		
LD	dB	dBm	NÚMERO DE FÓTONS		dBm	NÚMERO DE FÓTONS	
			1,642 µW	1,542 µW		1,642 µW	1,542 µW
ON	21	-90.334	78.2328	73.4683	-89.566	67.8018	63.6725
ON	25	-93.819	31.1450	29.2483	-93.247	26.9924	25.3485
ON	30	-97.083	9.8489	9.2491	-99.544	8.5357	8.0159
ON	35	-101.511	3.1145	2.9248	-104.769	2.6992	2.5348
ON	40	-107.350	0.9849	0.9249	-107.377	0.8536	0.8016
ON	45	-111.867	0.3115	0.2925	-111.442	0.2699	0.2535
ON	46	-113.485	0.2474	0.2323	-112.559	0.2144	0.2014

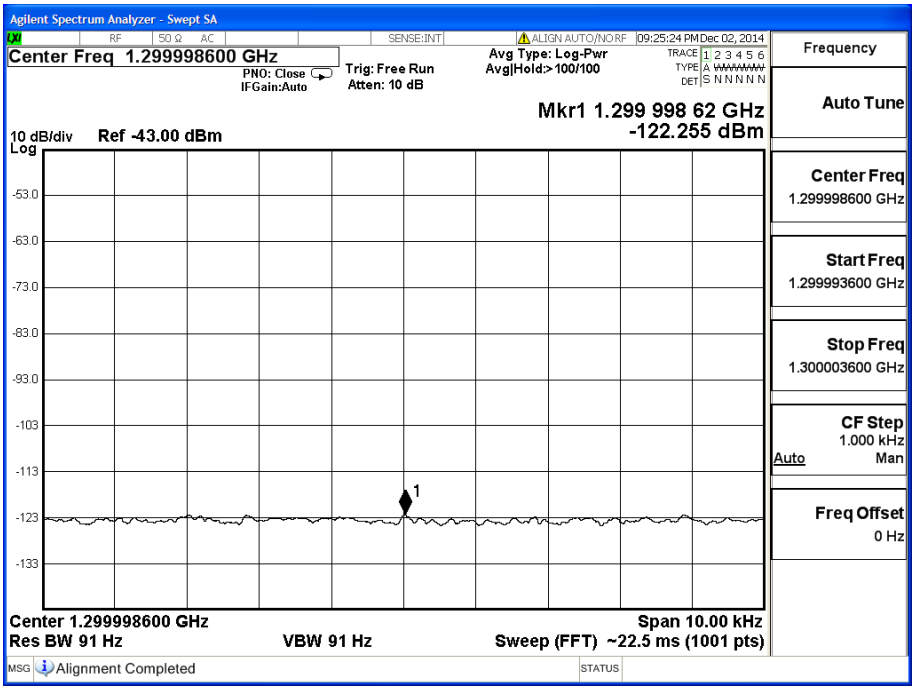
continua

FREQUÊNCIA		1.3 GHz			1.5 GHz		
LD	dB	dBm	NÚMERO DE FÓTONS		dBm	NÚMERO DE FÓTONS	
			1,642 µW	1,542 µW		1,642 µW	1,542 µW
ON	47	-114.339	0.1965	0.1845	-113.790	0.1703	0.1599
ON	48	-114.885	0.1561	0.1466	-114.385	0.1353	0.1270
ON	49	-115.468	0.1240	0.1164	-114.873	0.1075	0.1009
ON	50	-116.461	0.0985	0.0925	-116.561	0.0854	0.0802
ON	51	-116.869	0.0782	0.0735	-117.045	0.0678	0.0637
ON	52	-117.398	0.0621	0.0584	-117.779	0.0539	0.0506
ON	53	-118.200	0.0494	0.0464	-117.840	0.0428	0.0402
ON	54	-119.394	0.0392	0.0368	-118.659	0.0340	0.0319
ON	55	-120.240	0.0311	0.0292	-120.126	0.0270	0.0253
ON	60	-122.292	0.0098	0.0092	-121.225	0.0085	0.0080
OFF	X	-122.758	0	0	-121.800	0	0

Fonte: elaborada pelo autor.

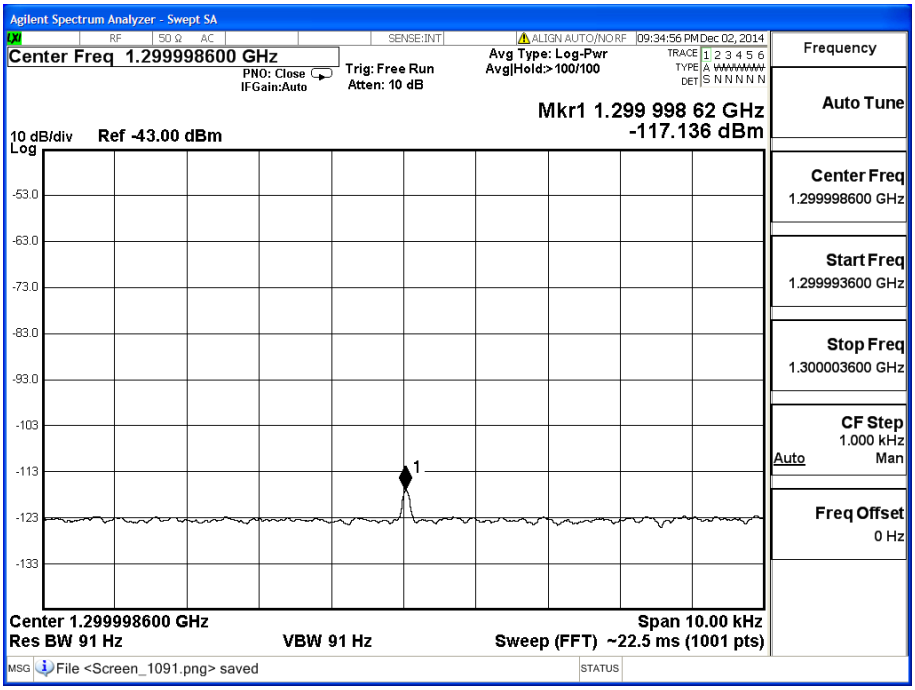
A Tabela 5 mostra os valores de atenuação óptica utilizados, a potência elétrica medida pelo analisador de espectro, e o respectivo número médio de fótons para essa potência. Mostra-se também, como referência, o valor da potência no analisador de espectro quando o laser está desligado, ou seja, há apenas o ruído de fundo. As FIGURAS 16 e 17 apresentam, respectivamente, a tela do analisador de espectro quando o laser está desligado e quando um sinal modulante de 1,3 GHz alimenta o modulador de amplitude, com uma atenuação óptica de 50 dB no braço do sinal (o que dá $n \sim 0{,}1$).

Figura 16 – Tela do analisador de espectro com o laser desligado.



Fonte: elaborada pelo autor.

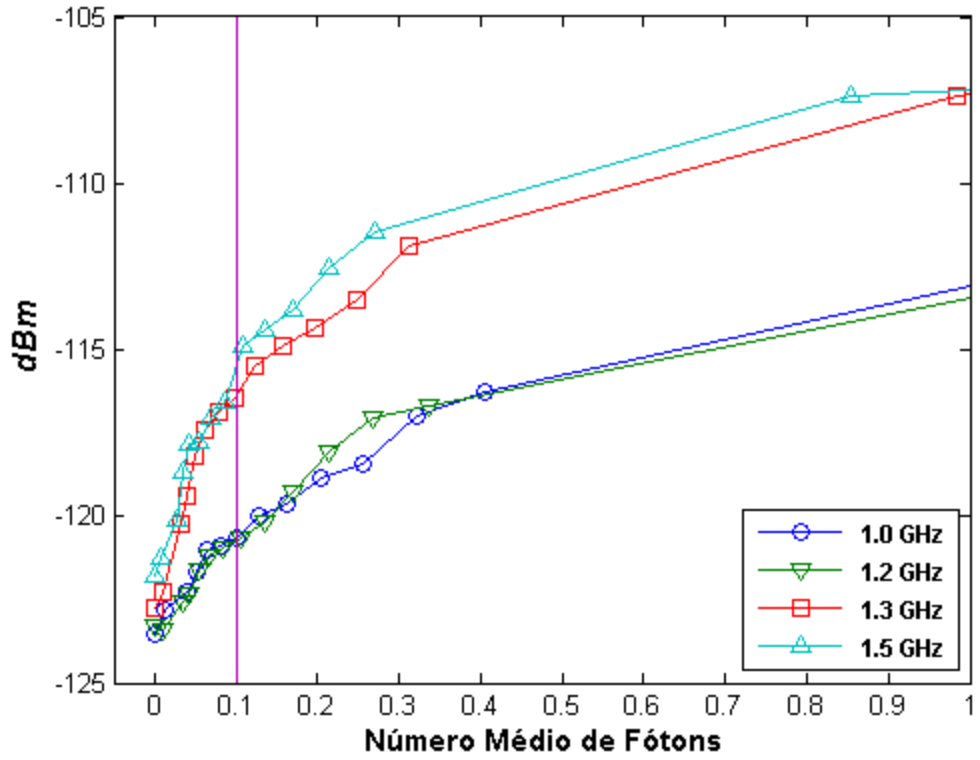
Figura 17 – Tela do analisador de espectro quando um sinal modulante de 1,3 GHz é utilizado com atenuação de 50 dB e número médio de fótons de 0,0985.



Fonte: elaborada pelo autor.

A FIGURA 18 mostra a curva potência elétrica medida no analisador de espectro versus o número médio de fótons calculado a partir do valor de potência medida, para as quatro frequências consideradas.

Figura 18 – Potência versus número médio de fótons.



Fonte: elaborada pelo autor.

7 POLARIZAÇÃO QUÂNTICA DE ESTADOS CONTÍNUOS DA LUZ

7.1 Parâmetros de Stokes Quântico

A polarização da luz é uma propriedade que pode ter aplicações diversas em comunicação e computação quânticas. Embora, de certa forma, a polarização tenha uma definição simples baseada na trajetória descrita pelo vetor campo elétrico, quando estados quânticos da luz são considerados, a definição se torna mais complexa e o grau de polarização, ou seja, o quanto a luz é polarizada, passa a depender do número de fótons do estado.

Um estado coerente polarizado pode ser convenientemente representado como um estado coerente de dois modos, ou dois estados coerentes de modo único em direções ortogonais. As variáveis que determinam completamente as propriedades de polarização do campo eletromagnético clássico são conhecidas como parâmetros de Stokes e seus análogos mecânicos quânticos, os operadores de Stokes (hermitianos) são ferramentas adequadas para a descrição da polarização quântica de estados contínuos da luz. Três dos quatro operadores de Stokes não se deslocam, apresentando entre eles as bem conhecidas relações de incerteza (KOROLKOVA *et al*. 2002).

De fato, qualquer par de variáveis contínuas quânticas que não comutam (quadraturas, variáveis de polarização) seria adequada para um protocolo de distribuição de chave quântica de variável contínua. Os valores esperados, bem como as variâncias dos operadores de Stokes, podem ser facilmente medidos usando dispositivos ópticos lineares e fotodiodos PIN, sem a necessidade de um oscilador local separado e detectores de fótons individuais (AGARWAL; CHATURVEDI, 2003; KOROLKOVA *et al*. 2002).

Este capítulo objetiva propor uma nova medida do grau de polarização da luz baseada na entropia de Shannon, bem como calcular o grau de polarização de estados de um fóton e coerentes contínuos. As ferramentas adequadas para o tratamento matemático da polarização quântica podem ser encontradas na literatura (BARRANCO; BORELLI, 2006; CHIRKIN *et al*., 1993; USACHEV *et al*., 2001; AGARWAL *et al*., 1996; PRAKASH; CHANDRA, 1971). A versão quântica dos parâmetros de Stokes é a seguinte:

$$\hat{S}_0 = \hat{a}_1^\dagger \hat{a}_1 + \hat{a}_2^\dagger \hat{a}_2, \tag{7.1}$$

$$\hat{S}_1 = \hat{a}_1^\dagger \hat{a}_1 - \hat{a}_2^\dagger \hat{a}_2, \tag{7.2}$$

$$\hat{S}_2 = \hat{a}_1^\dagger \hat{a}_2 + \hat{a}_2^\dagger \hat{a}_1, \tag{7.3}$$

$$\hat{S}_3 = i\left(\hat{a}_2^\dagger \hat{a}_1 - \hat{a}_1^\dagger \hat{a}_2\right), \tag{7.4}$$

$$\left[\hat{S}_2, \hat{S}_3\right] = i2\hat{S}_1. \tag{7.5}$$

Um campo óptico pode ser considerado despolarizado se suas propriedades observáveis, os parâmetros de Stokes, permanecerem inalteradas após a aplicação de uma rotação geométrica, $R_\theta = exp(i\theta\hat{S}_3)$, e/ou um deslocamento de fase entre as duas componentes linearmente polarizadas (modos horizontal e vertical), $C_\varphi = exp(i0{,}5\varphi\hat{S}_1)$. Estas condições são descritas matematicamente por $[\rho_{unpol},\ \hat{S}_3] = [\rho_{unpol},\ \hat{S}_1] = 0$, sendo ρ_{unpol} a matriz densidade do estado despolarizado (LEHNER *et al*., 1996; SÖDERHOLM *et al*., 2001). A forma mais geral de uma luz despolarizada é dada por (SILVA; RAMOS, 2008; SÖDERHOLM *et al*., 2001):

$$\rho_{unpol} = \sum_n p_n \frac{1}{n+1} \sum_{k=0}^{n} |k\rangle|n-k\rangle\langle k|\langle n-k|. \tag{7.6}$$

Qualquer medida de grau de polarização aplicada à matriz densidade ρ_{unpol} deve retornar um valor nulo. Em (7.6) p_n é a distribuição de probabilidade do número de fótons considerando ambos os modos, horizontal e vertical. Existem algumas propostas para o grau de polarização quântico, (*Degree Of Polarization* – DOP). A primeira tentativa de quantificar a polarização quântica da luz foi proposta por Luis usando a função *Q* baseada em estados coerentes em SU(2) (LUIS, 2002):

$$Q(\theta,\varphi)=\sum_{n=0}^{\infty}\frac{n+1}{4\pi}\langle n,\theta,\varphi|\rho|n,\theta,\varphi\rangle, \tag{7.7}$$

$$|n,\theta,\varphi\rangle=\sum_{m=0}^{n}\binom{n}{m}^{1/2}\left[\sin\left(\frac{\theta}{2}\right)\right]^{n-m}\left[\cos\left(\frac{\theta}{2}\right)\right]^{m}e^{-im\varphi}|m\rangle|n-m\rangle. \tag{7.8}$$

O DOP é então dado por:

$$D=4\pi\int\left[Q(\theta,\varphi)-\frac{1}{4\pi}\right]^{2}\sin(\theta)\,d\theta d\varphi, \tag{7.9}$$

$$G_Q=\frac{D}{1+D}\qquad 0\le G_Q\le 1. \tag{7.10}$$

Sendo que $1/(4\pi)$ é a função *Q* da luz despolarizada dada em (7.6). Como pode ser notada, esta medida é baseada na distância entre a pseudodistribuição[2] (função *Q*) da luz cuja polarização se deseja medir e a pseudodistribuição da luz despolarizada. Existem outras medidas de DOP baseadas em distância, por exemplo, a distância de Hilbert-Schmidt entre duas matrizes (KLIMOV *et al*., 2005):

$$D_{HS}\left(\rho,\rho_{unpol}\right)=\left\|\rho-\rho_{unpol}\right\|^{2}=Tr\left[\left(\rho-\rho_{unpol}\right)^{2}\right], \tag{7.11}$$

$$\rho_{unpol}=\sum_{n=0}^{\infty}\sum_{k=0}^{n}\frac{\langle k,n-k|\rho|k,n-k\rangle \mathrm{I}_n}{n+1}. \tag{7.12}$$

[2] A função Q deveria funcionar como uma distribuição de probabilidade ao longo da esfera de Poincaré. Por exemplo, para o estado despolarizado a função Q é $1/4\pi$ indicando que todas as polarizações, para um estado despolarizado, são igualmente prováveis. Lembre-se que a área de esfera é $4\pi R^2$, só que o raio da esfera de Poincaré é 1, logo, $1/4\pi$ é uma distribuição uniforme na esfera. Acontece que, para outros estados quânticos, a função pode assumir valores negativos ou até infinito. Nesses casos a tentativa de associá-la a uma distribuição de probabilidade (dos possíveis estados de polarização) não faz sentido, pois uma distribuição de probabilidade é sempre positiva e sem singularidades. Enfim, como as vezes pode-se associar a função Q a uma distribuição e outras vezes não (depende do estado quântico), ela (e muitas outras pelo mesmo motivo, como a função P e a de Wigner) é dita ser uma pseudodistribuição.

7.2 Grau de Polarização Baseado na Entropia de Shannon

Do ponto de vista experimental, determina-se a polarização da luz através da medição dos parâmetros de Stokes. Por isso, parece natural que o DOP deve refletir a incerteza dos resultados dessas medições. Nessa direção, a presente seção propõe uma fórmula para o DOP com base nas entropias das distribuições dos resultados das medições dos parâmetros de Stokes. Para um estado de luz de dois modos com matriz de densidade ρ, o DOP baseado na entropia é dado por:

$$G(\rho) = 1 - \min_{\phi,\theta,\varepsilon} \frac{E\left(\text{Prob}_{S_1}\left(U_{\phi\theta\varepsilon}\rho U_{\phi\theta\varepsilon}^{\dagger}\right)\right) E\left(\text{Prob}_{S_2}\left(U_{\phi\theta\varepsilon}\rho U_{\phi\theta\varepsilon}^{\dagger}\right)\right) E\left(\text{Prob}_{S_3}\left(U_{\phi\theta\varepsilon}\rho U_{\phi\theta\varepsilon}^{\dagger}\right)\right)}{\left[E\left(\text{Prob}_{S_1}\left(\rho_{unpol}\right)\right)\right]^3}, \quad (7.13)$$

$$U_{\phi\theta\varepsilon} = C_{\phi} R_{\theta} C_{\varepsilon}. \quad (7.14)$$

Em (7.13) E é a entropia de Shannon, $Prob_{Si}$ é a distribuição de probabilidade dos resultados da medição de S_i e ρ_{unpol} é o estado despolarizado mais próximo de ρ dado por (7.12). De (7.13), pode-se ver imediatamente que $G(\rho) = 0$ para qualquer ρ despolarizado. Por outro lado, $G(\rho) = 1$ se uma das distribuições de probabilidades é uma função delta, isto é, a medição de um dos parâmetros de Stokes dá sempre o mesmo resultado. Por exemplo, os estados $|1,\ 0\rangle_{HV}$ e $\cos(\theta)\,|1,\ 0\rangle_{HV} + \text{sen}(\theta)\,|0,\ 1\rangle_{HV}$ têm $G = 1$, uma vez que S_1 é sempre igual a 1 para o primeiro e o último é apenas uma rotação do primeiro (ρ e $U_{\phi\theta\varepsilon}\rho U_{\phi\theta\varepsilon}^{\dagger}$ devem ter o mesmo valor para o DOP). Seja agora o seguinte estado misto de um fóton,

$$\rho = (1-\xi)\frac{\left[|0\ 1\rangle\langle 0\ 1| + |1\ 0\rangle\langle 1\ 0|\right]_{HV}}{2} + \xi|\psi\rangle\langle\psi|, \quad (7.15)$$

$$|\psi\rangle = \cos(\lambda)|1\ 0\rangle_{HV} + e^{i\mu}\sin(\lambda)|0\ 1\rangle_{HV}, \quad (7.16)$$

Calculando o DOP usando (7.13) obtêm-se

$$G = 1 - \frac{\left[(1-\xi)/2\right]\log\left((1-\xi)/2\right) + \left[(1+\xi)/2\right]\log\left((1+\xi)/2\right)}{\log(1/2)}. \tag{7.17}$$

Como esperado em (7.17) $G(\xi = 0) = 0$ e $G(\xi = 1) = 1$. Para o estado de dois fótons,

$$\rho = \xi\left[\frac{|2\ 0\rangle\langle 2\ 0| + |1\ 1\rangle\langle 1\ 1| + |0\ 2\rangle\langle 0\ 2|}{3}\right] + (1-\xi)|\psi\rangle\langle\psi|, \tag{7.18}$$

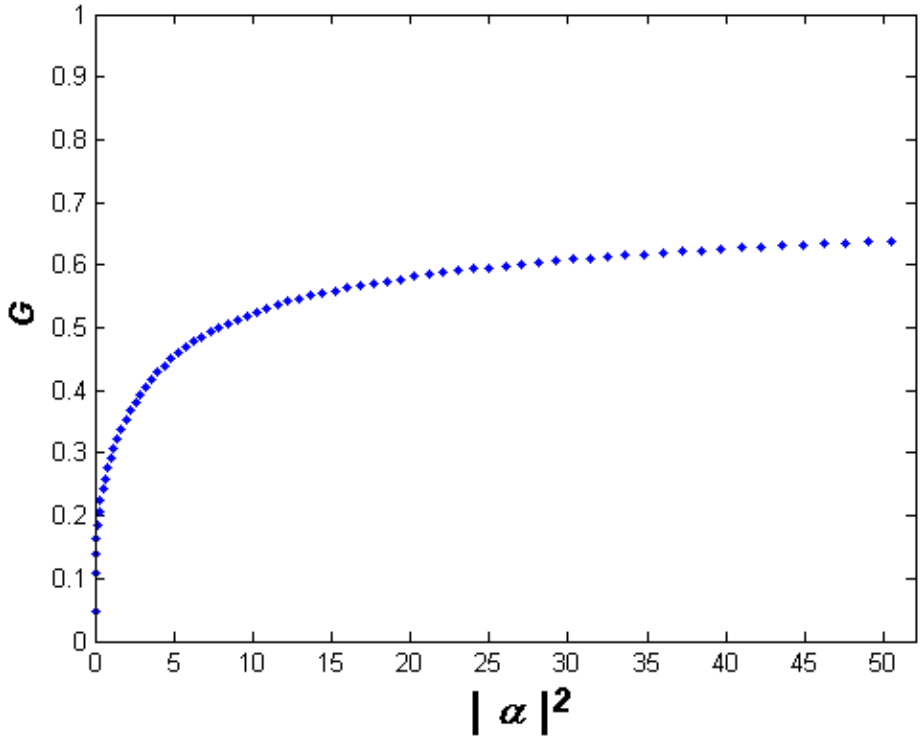
$$|\psi\rangle = \text{sen}(2\theta)\left(\frac{|0\ 2\rangle - |2\ 0\rangle}{\sqrt{2}}\right) + \cos(2\theta)|1\ 1\rangle,$$

o DOP baseado na entropia é dado por:

$$G(\rho) = 1 - \frac{\left[\left(\frac{2-2\xi}{3}\right)\log\left(\frac{1-\xi}{3}\right) + \left(\frac{1+2\xi}{3}\right)\log\left(\frac{1+2\xi}{3}\right)\right]\left[\left(\frac{2+\xi}{3}\right)\log\left(\frac{2+\xi}{6}\right) + \left(\frac{1-\xi}{3}\right)\log\left(\frac{1-\xi}{3}\right)\right]^2}{\left[\log\left(\frac{1}{3}\right)\right]^3}. \tag{7.20}$$

Como esperado em (7.20) $G(\xi = 0) = 0$ e $G(\xi = 1) = 1$. Para o estado coerente de dois modos $|\lambda,\ \beta\rangle$ pode-se sempre encontrar uma transformação $U_{\phi\theta\varepsilon}$, tal que $U_{\phi\theta\varepsilon}|\lambda,\ \beta\rangle = |\alpha, 0\rangle$ e $|\alpha|^2 = |\lambda|^2 + |\beta|^2$. Como $U_{\phi\theta\varepsilon}$ não muda o DOP, basta calcular $G(|\alpha, 0\rangle)$. Para este cálculo usamos para ρ_{unpol} em (7.13) a equação (7.6) com $P_n = exp(-|\alpha|^2)(|\alpha|^2)^n/n!$. Neste caso, a distribuição de probabilidades para S_i é uma distribuição Poissoniana com valor médio e variância igual a $|\alpha|^2$, enquanto que as distribuições de probabilidades para S_2 e S_3 são distribuições de Skellam com valor médio igual a zero e variância igual a $|\alpha|^2$. Um cálculo numérico de $G(|\alpha, 0\rangle)$ para $|\alpha|^2$ variando no intervalo [0,001, 50] pode ser visto na FIGURA 19.

Figura 19 – Grau de polarização do estado coerente de dois modos $|\alpha, 0\rangle$ versus $|\alpha|^2$.



Fonte: elaborada pelo autor.

Como esperado para estados coerentes de dois modos, o DOP aumenta com o número médio de fótons. No entanto, diferentemente do DOP de $|\alpha, 0\rangle$ usando as equações (7.9) e (7.10), ele nunca atinge o valor máximo $G = 1$, uma vez que a distribuição de probabilidade dos parâmetros de Stokes não tende a uma função delta quando a potência óptica aumenta.

7.3 Polarização de Estados Quânticos Contínuos da Luz

Os estados coerentes contínuos foram utilizados no Capítulo 1 para aumentar a segurança de protocolos de comunicação quântica segura direta. Nesta seção o objetivo é calcular o DOP para estados contínuos coerentes e de um fóton. Para isso, inicialmente é feita a discretização do estado contínuo (GUERRA *et al*., 2016; RAMOS; SOUSZA, 2001; RIOS *et al*., 2017). A discretização dos estados contínuo de um fóton e de estados coerentes é dada na seção 4.

$$\left|1_{\omega}\right\rangle=\int_{0}^{\infty}\sigma\left(\omega\right)\hat{a}^{+}\left(\omega\right)d\omega\left|0_{\omega}\right\rangle\approx\sum_{k=1}^{N}\sigma\left(k\omega_{s}\right)\sqrt{\omega_{s}}\left|0\right\rangle_{1}...\left|1\right\rangle_{k}...\left|0\right\rangle_{N}=\sum_{k=1}^{N}\sigma\left(k\omega_{s}\right)\sqrt{\omega_{s}}\left|\tilde{1}\right\rangle_{k},\qquad(7.21)$$

$$\sum_{k=1}^{N}\left|\sigma\left(k\omega_{s}\right)\right|^{2}\omega_{s}=1\qquad(7.22)$$

$$\left|\alpha_{\omega}\right\rangle=\exp\left[\int\left[\alpha\left(\omega\right)a^{\dagger}\left(\omega\right)-\alpha^{*}\left(\omega\right)a\left(\omega\right)\right]d\omega\right]\left|0_{\omega}\right\rangle=\prod_{k=1}^{N}\left|\alpha\left(k\omega_{s}\right)\sqrt{\omega_{s}}\right\rangle,\qquad(7.23)$$

$$\left\langle n\right\rangle=\sum_{k=1}^{N}\left|\alpha\left(k\omega_{s}\right)\right|^{2}\omega_{s}.\qquad(7.24)$$

Em (7.21) $|\sigma(\omega)|^2 d\omega$ dá a probabilidade da frequência do fóton pertencer ao intervalo $(\omega,\ \omega+d\omega)$. Além disso, em (7.23) e (7.24) ω_s é o passo de discretização no domínio da frequência. Assim, $\sigma(k\omega_s)$ é o valor de $\sigma(\omega)$ em $\omega = k\omega_s$ sendo *k* um número inteiro. Como se pode notar em (7.21), o estado contínuo de fótons únicos é aproximado por uma superposição do produto tensorial de osciladores discretos onde cada oscilador discreto trabalha em uma única frequência. Por exemplo, o estado $\left|\tilde{1}\right\rangle_k = |0\rangle_1 \cdots |1\rangle_k \cdots |0\rangle_N$ significa um fóton na frequência $k\omega_s$ e zero fótons nas outras frequências. O número de osciladores discretos *N* é igual ao número de amostras de $\sigma(\omega)$ e a amplitude de probabilidade do *k*-ésimo termo na superposição é dada por $\sigma(k\omega_s)(\omega_s)^{1/2}$.

Por outro lado, (7.23) mostra que o estado coerente contínuo pode ser aproximado por um produto tensorial de estados coerentes de uma única frequência com amplitude $\sigma(k\omega_s)(\omega_s)^{1/2}$ na frequência $\omega = k\omega_s$.

7.4 Grau de Polarização de Campos Contínuos e Canais Despolarizantes

Considera-se primeiramente o estado contínuo de um fóton sendo propagado em um canal com ruído de fase dependente da frequência como discutido em (BERGLUND, 2000; GONG *et al*., 2008). O estado na entrada do canal é

$$|\psi\rangle = |1_\omega\rangle \otimes \left(a|\lambda_1\rangle + b|\lambda_2\rangle\right) = \sum_{k=1}^{N} \sigma(k\omega_s)\sqrt{\omega_s}\,|\tilde{1}\rangle_k \otimes \left(a|\lambda_1\rangle + b|\lambda_2\rangle\right). \tag{7.25}$$

Onde λ_1 e λ_2 são os modos horizontal e vertical. Portanto, para o estado inicial frequência e polarização são independentes, ou seja, não estão entrelaçadas. O efeito da propagação no canal é modelado pelo operador unitário $U_m(\omega) = \lambda_1^m(\omega)|\lambda_1\rangle\langle\lambda_1| + \lambda_2^m(\omega)|\lambda_2\rangle\langle\lambda_2|$, com probabilidade p_m (os autovalores dependem da frequência e de uma variável aleatória, mas os autoestados são constantes). Portanto, o estado na saída do canal é

$$\rho_{out} = \sum_m p_m |\psi_m\rangle\langle\psi_m| = \sum_m p_m \rho_m, \tag{7.26}$$

$$|\psi_m\rangle = \sum_{k=1}^{N} \sigma(k\omega_s)\sqrt{\omega_s}\,|\tilde{1}\rangle_k\, U_m\left(a|\lambda_1\rangle + b|\lambda_2\rangle\right) = \sum_{k=1}^{N} \sigma(k\omega_s)\sqrt{\omega_s}\,|\tilde{1}\rangle_k \left(a\lambda_1^m(k\omega_s)|\lambda_1\rangle + b\lambda_2^m(k\omega_s)|\lambda_2\rangle\right), \tag{7.27}$$

$$\rho_m = \sum_{k,l=1}^{N} \sigma(k\omega_s)\sigma^*(l\omega_s)\omega_s\,|\tilde{1}\rangle_{k\ l}\langle\tilde{1}| \otimes \begin{pmatrix} |a|^2 \lambda_1^m(k\omega_s)\left(\lambda_1^m(l\omega_s)\right)^* |\lambda_1\rangle\langle\lambda_1| + |b|^2 \lambda_2^m(k\omega_s)\left(\lambda_2^m(l\omega_s)\right)^* |\lambda_2\rangle\langle\lambda_2| \\ +ab^*\lambda_1^m(k\omega_s)\left(\lambda_2^m(l\omega_s)\right)^* |\lambda_1\rangle\langle\lambda_2| + a^*b\left(\lambda_1^m(l\omega_s)\right)^* \lambda_2^m(k\omega_s)|\lambda_2\rangle\langle\lambda_1| \end{pmatrix}. \tag{7.28}$$

Pode-se observar em (7.28) que polarização e frequência agora estão entrelaçados. Para obter a informação apenas sobre a polarização, a variável correspondente à frequência é traçada fora em (7.28). Usando $Tr_\omega\left(|\tilde{1}\rangle_k\ {}_l\langle\tilde{1}|\right) = {}_l\langle\tilde{1}|\tilde{1}\rangle_k = \delta_{kl}$ e (7.22) obtêm-se para o estado de polarização na saída do canal

$$\rho_m = \begin{bmatrix} |a|^2 & ab^*\sum_{k=1}^{N} |\sigma(k\omega_s)|^2 \omega_s \lambda_1^m(k\omega_s)\left(\lambda_2^m(k\omega_s)\right)^* \\ a^*b\sum_{k=1}^{N} |\sigma(k\omega_s)|^2 \omega_s \left(\lambda_1^m(k\omega_s)\right)^* \lambda_2^m(k\omega_s) & |b|^2 \end{bmatrix}. \tag{7.29}$$

$$\rho_{out} = \sum_m p_m \rho_m = \begin{bmatrix} |a|^2 & ab^* \sum_m p_m \sum_{k=1}^{N} \left|\sigma(k\omega_s)\right|^2 \omega_s \lambda_1^m(k\omega_s)\left(\lambda_2^m(k\omega_s)\right)^* \\ a^* b \sum_m p_m \sum_{k=1}^{N} \left|\sigma(k\omega_s)\right|^2 \omega_s \left(\lambda_1^m(k\omega_s)\right)^* \lambda_2^m(k\omega_s) & |b|^2 \end{bmatrix}. \quad (7.30)$$

Como mostrado em (7.30), os elementos na diagonal da matriz densidade não mudam. A Equação (7.30) pode ser reescrita como

$$\rho_{out} = (1-\xi)\frac{I}{2} + \xi \begin{bmatrix} \frac{|a|^2 - |b|^2}{2\xi} + \frac{1}{2} & \frac{ab^* \sum_m p_m \sum_{k=1}^{N} \left|\sigma(k\omega_s)\right|^2 \omega_s \lambda_1^m(k\omega_s)\left(\lambda_2^m(k\omega_s)\right)^*}{\xi} \\ \frac{a^* b \sum_m p_m \sum_{k=1}^{N} \left|\sigma(k\omega_s)\right|^2 \omega_s \left(\lambda_1^m(k\omega_s)\right)^* \lambda_2^m(k\omega_s)}{\xi} & -\frac{|a|^2 - |b|^2}{2\xi} + \frac{1}{2} \end{bmatrix}, \quad (7.31)$$

e, portanto, o grau de polarização depende somente do parâmetro ξ dado por

$$\xi = \sqrt{1 - 4\det(\rho)} = \sqrt{1 - 4|a|^2|b|^2\left[1 - \sum_{m,q} p_i p_j \sum_{k,l=1}^{N} \left|\sigma(k\omega_s)\right|^2 \left|\sigma(l\omega_s)\right|^2 \omega_s^2 \lambda_1^m(k\omega_s)\left(\lambda_2^m(k\omega_s)\right)^* \left(\lambda_1^q(l\omega_s)\right)^* \lambda_2^q(l\omega_s)\right]}. \quad (7.32)$$

Assumindo autovalores da forma

$$\lambda_{1,2}^m(k\omega_s) = e^{i\left(\frac{n_{1,2} k\omega_s L}{c} + \phi_m^{1,2}\right)}, \quad (7.33)$$

onde $n_{1,2}$ são os índices de refração nos eixos ópticos ortogonais, $\phi_m^{1,2} \in [0, 2\pi]$ é uma variável aleatória com distribuição p_m e L é o comprimento do canal, o parâmetro ξ fica na forma

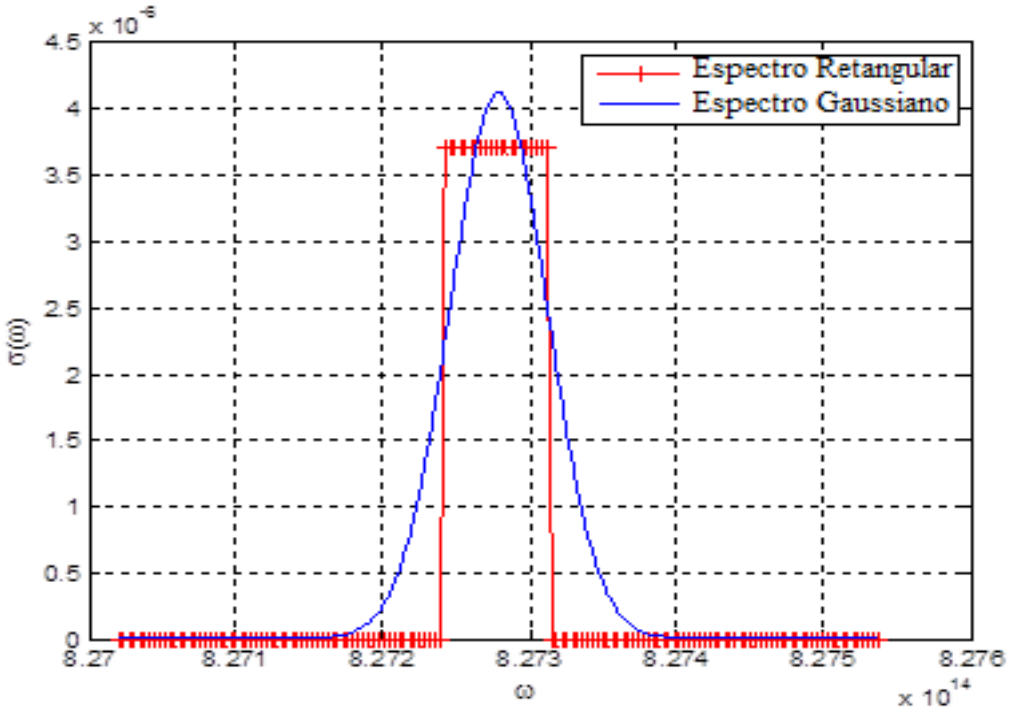
$$\xi = \sqrt{1-4|a|^2|b|^2\left[1-\sum_{m,q} p_m p_q e^{i\left[\left(\phi_m^1-\phi_m^2\right)-\left(\phi_q^1-\phi_q^2\right)\right]} \sum_{k,l=1}^{N} \left|\sigma(k\omega_s)\right|^2 \left|\sigma(l\omega_s)\right|^2 \omega_s^2 e^{i\left(\frac{(n_1-n_2)(k-l)\omega_s L}{c}\right)}\right]}. \quad (7.34)$$

Em um primeiro momento, sem considerar as variáveis aleatórias, a despolarização é toda devido à largura espectral do campo e à dependência das propriedades do canal com a frequência. Neste caso tem-se

$$\xi = \sqrt{1-4|a|^2|b|^2\left[1-\sum_{k,l=1}^{N} \left|\sigma(k\omega_s)\right|^2 \left|\sigma(l\omega_s)\right|^2 \omega_s^2 e^{i\left(\frac{(n_1-n_2)(k-l)\omega_s L}{c}\right)}\right]}. \quad (7.35)$$

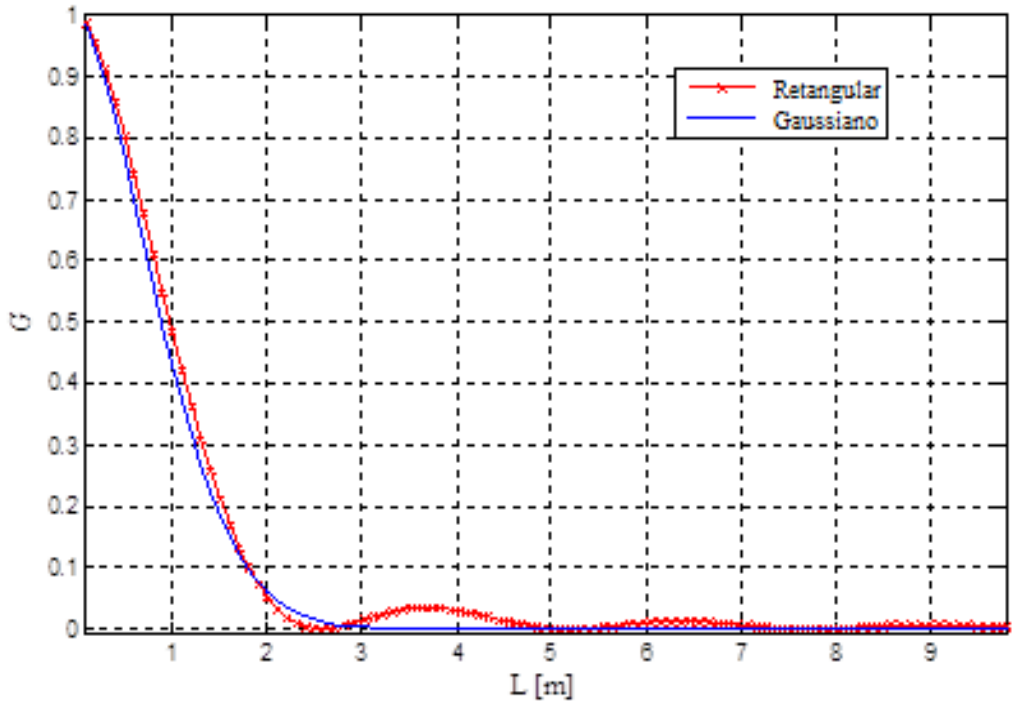
O cálculo numérico de DOP, usando (7.17) e (7.35), para os espectros Gaussiano e retangular mostrados na FIGURA 20 podem ser vistos na FIGURA 21.

Figura 20 – Espectros retangular e gaussiano.



Fonte: elaborada pelo autor.

Figura 21 – Grau de polarização (*G*) usando Eq. (7.17) versus comprimento do canal (*L*), para os campos com espectro gaussiano (-) e retangular (+).



Fonte: elaborada pelo autor.

Nesta simulação numérica os seguintes valores de parâmetros foram utilizados: $N = 150$, $n_1 = 1{,}47$, $n_2 = 1{,}46$, $\omega_c = 2\pi c/(n_1 \times 1550\text{nm})$, $\omega_{min} = \omega_c - (0.258 \times 10^6)$, $\omega_{max} = \omega_c + (0.258 \times 10^6)$, $\omega_s = (\omega_{max} - \omega_{min})/(N-1)$, $|\alpha|^2 = |\beta|^2 = 1/2$.

Agora, considera-se (7.34) e assume-se que $\phi_1^1 - \phi_1^2 = 0$ com probabilidade $p_1 = 1/2$ e $\phi_2^1 - \phi_2^2 = \pi$ com probabilidad $p_2 = 1/2$. Neste caso, para $|\alpha|^2 = |\beta|^2 = 1/2$ tem-se $\xi = 0$, o que implica em $G = 0$, independentemente da distribuição espectral do fóton. De fato, a introdução da variável aleatória torna o canal mais fortemente despolarizante.

Para estados coerente contínuos de dois modos tem-se:

$$\left|\alpha_\omega, \beta_\omega\right\rangle = \prod_{k=1}^{N} \left|\alpha(k\omega_s)\sqrt{\omega_s}\right\rangle \otimes \prod_{k=1}^{N} \left|\beta(k\omega_s)\sqrt{\omega_s}\right\rangle, \tag{7.36}$$

Usando a função *Q* para o cálculo do grau de polarização, tem-se a seguinte fórmula:

$$G = \frac{1}{P_T}\sum_{k=1}^{N} P_k \times G_{individual}\left(\left|\alpha(\omega_k), \beta(\omega_k)\right\rangle\right), \tag{7.37}$$

$$P_k = \left|\alpha(\omega_k)\right|^2 + \left|\beta(\omega_k)\right|^2, \tag{7.38}$$

$$P_T = \sum_{k=1}^{N} P_k, \tag{7.39}$$

$$G_{individual}\left(\left|\alpha(\omega_k), \beta(\omega_k)\right\rangle\right) = 1 - \frac{4P_k}{\left(1 + 2P_k\left(1 + P_k\right)\right) - \exp\left(-2P_k\right)}. \tag{7.40}$$

Ou seja, o grau de polarização do estado coerente de várias frequências é igual à média dos graus de polarização em cada frequência ponderada pela potência de cada oscilador. Como o grau de polarização em (7.37) depende só da potência óptica, ele não varia com rotações geométricas ou variação da fase relativa entre as componentes ortogonais.

Para o cálculo numérico do grau de polarização de $|\alpha_\omega, \beta_\omega\rangle$ consideramos as seguintes distribuições espectrais Gaussianas:

$$\alpha(k\omega_s)\sqrt{\omega_s} = \frac{A_\alpha}{b_\alpha}\exp\left(\frac{-\left(k\omega_s - \omega_0\right)^2}{4\pi {b_\alpha}^2}\right)\exp(j\phi)\sqrt{\omega_s}, \tag{7.41}$$

$$\beta(k\omega_s)\sqrt{\omega_s} = \frac{A_\beta}{b_\beta}\exp\left(\frac{-\left(k\omega_s - \omega_0\right)^2}{4\pi {b_\beta}^2}\right)\exp(j\phi)\sqrt{\omega_s}, \tag{7.42}$$

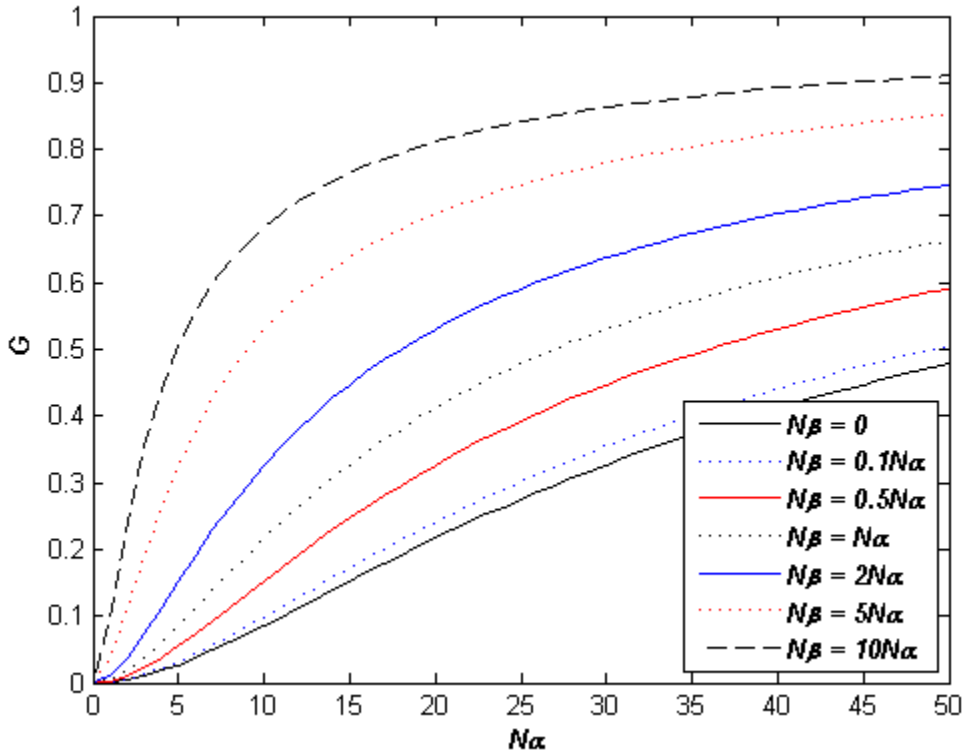
$$A_{\alpha,\beta} = \left(\frac{\left\langle N_{\alpha,\beta}\right\rangle b_{\alpha,\beta}}{\pi\sqrt{2}}\right)^{1/2}, \tag{7.43}$$

$$b_{\alpha,\beta} = \left[\left(2\pi T_{\alpha,\beta}{}^{2} \right)^{1/2} \right]^{-1}. \tag{7.44}$$

Os valores dos parâmetros são $\omega_0 = 2\pi \times 1.58061 \times 10^{14}$ rad/s, $\phi = \pi/3$, $T_{\alpha,\beta} = 5 \times 10^{-12} s$. A faixa de frequências consideradas é $[\omega_0 - \delta, \omega_0 + \delta]$ com $\delta = (60/(T_{\alpha,\beta})^2)^{1/2}$. O número de osciladores considerado é N_{osc} e o valor do passo no domínio da frequência é $2\delta/(N_{OSC} - 1)$. O parâmetro $\langle N_{\alpha,\beta} \rangle$ é o número médio de fótons.

A curva da simulação do grau de polarização dado em (7.37), para $N_{OSC} = 150$, versus o número médio de fótons pode ser visto na FIGURA 22.

Figura 22 – Grau de polarização (G) do estado coerente contínuo versus o número médio de fótons para 150 osciladores.

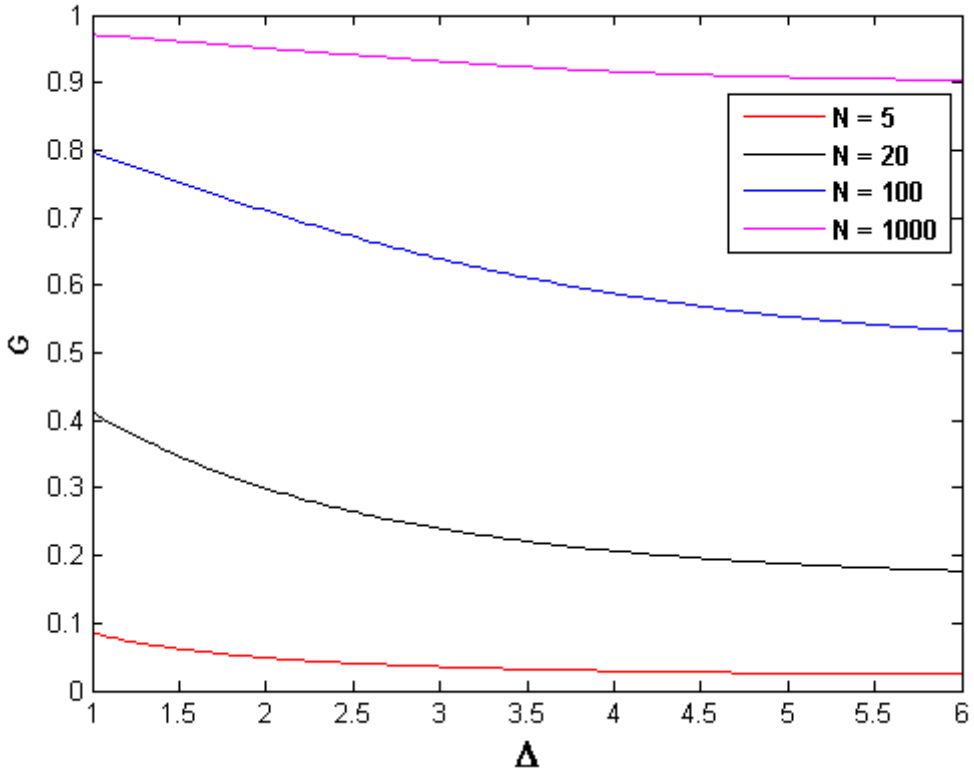


Fonte: elaborada pelo autor.

A curva da simulação do grau de polarização dado em (7.37) versus a largura do pulso β pode ser vista na FIGURA 23. Utilizou-se $N_{OSC} = 150$, $\langle N_\alpha \rangle = \langle N_\beta \rangle$ pertencentes ao conjunto {5, 20, 100, 1000}. Ou seja, a distribuição espectral de β passou a ser

$$\beta(k\omega_s)\sqrt{\omega_s} = \frac{A_\beta}{\Delta b_\beta}\exp\left(\frac{-(k\omega_s-\omega_0)^2}{4\pi\Delta^2 b_\beta{}^2}\right)\exp(j\phi)\sqrt{\omega_s}. \tag{7.45}$$

Figura 23 – Grau de polarização versus largura do pulso com 150 osciladores



Fonte: elaborada pelo autor.

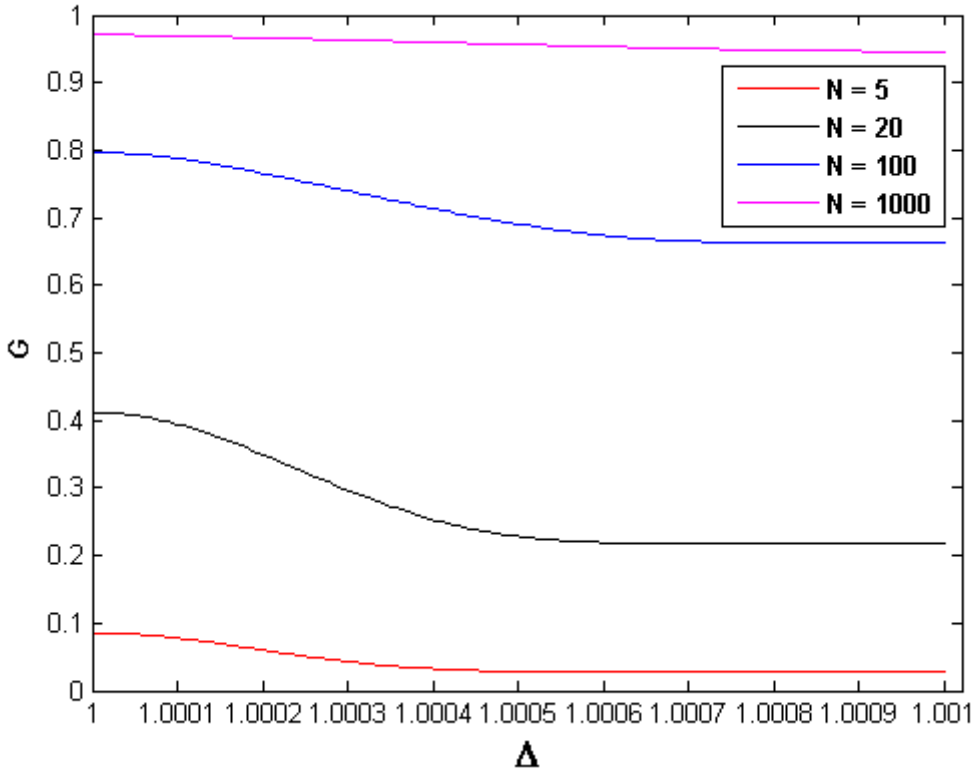
Observando as FIGURAS 22 e 23 pode-se notar que o grau de polarização é inversamente proporcional à largura do pulso e diretamente proporcional ao número médio de fótons. O alargamento no domínio da frequência (efeito que ocorre devido à meios dispersivos) , causa a diminuição da amplitude dos osciladores individuais o que, por sua vez, causa a diminuição do grau de polarização dos osciladores individuais.

Na FIGURA 24 tem-se o grau de polarização quando as distribuições espectrais α e β estão deslocadas na frequência. Ou seja, a distribuição espectral de β passou a ser

$$\beta(k\omega_s)\sqrt{\omega_s} = \frac{A_\beta}{b_\beta}\exp\left(\frac{-(k\omega_s-\Delta\omega_0)^2}{4\pi b_\beta{}^2}\right)\exp(j\phi)\sqrt{\omega_s}, \tag{7.46}$$

com Δ variando no intervalo [1, 1,001].

Figura 24 – Grau de polarização versus deslocamento do pulso Beta

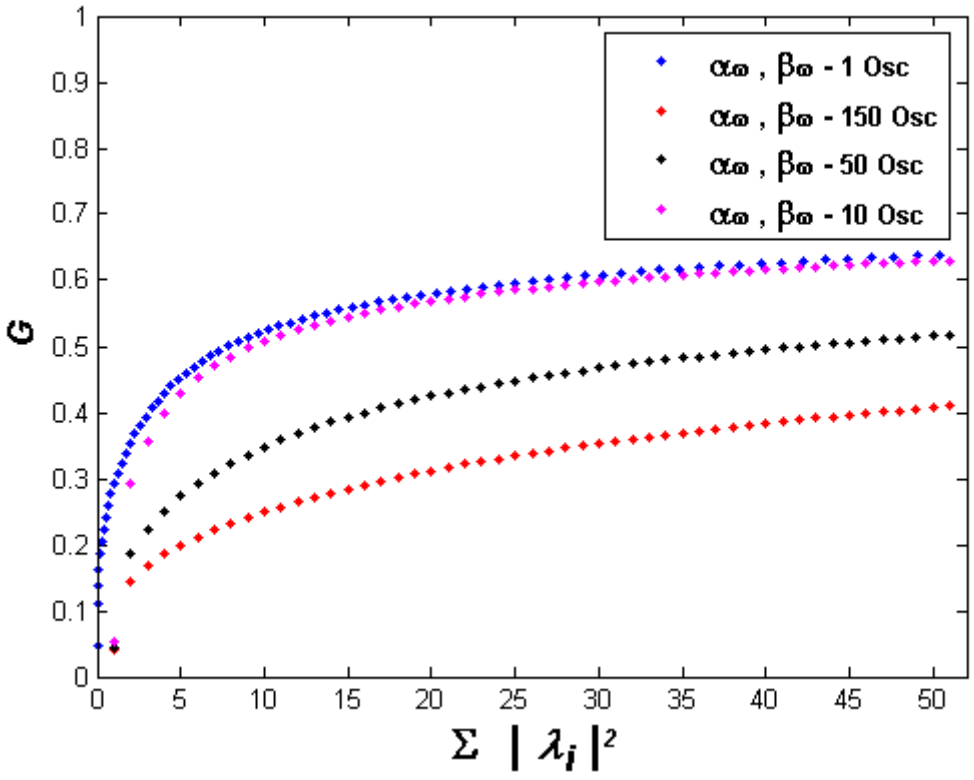


Fonte: elaborada pelo autor.

Novamente utilizou-se $N_{osc} = 150$ e $\langle N_\alpha \rangle = \langle N_\beta \rangle$ pertencentes ao conjunto {5, 20, 100, 1000}.

Por fim, a FIGURA 25 apresenta novamente o grau de polarização do estado $|\alpha_\omega, \beta_\omega\rangle$, usando a (7.37), mas agora usando como medida o grau de polarização de cada oscilador individual nas EQUAÇÕES (7.13) e (7.14).

Figura 25 – Grau de polarização versus número médio de fótons ($\langle N_\alpha \rangle + \langle N_\beta \rangle = |\lambda|^2$) para 150, 50 e 10 osciladores.

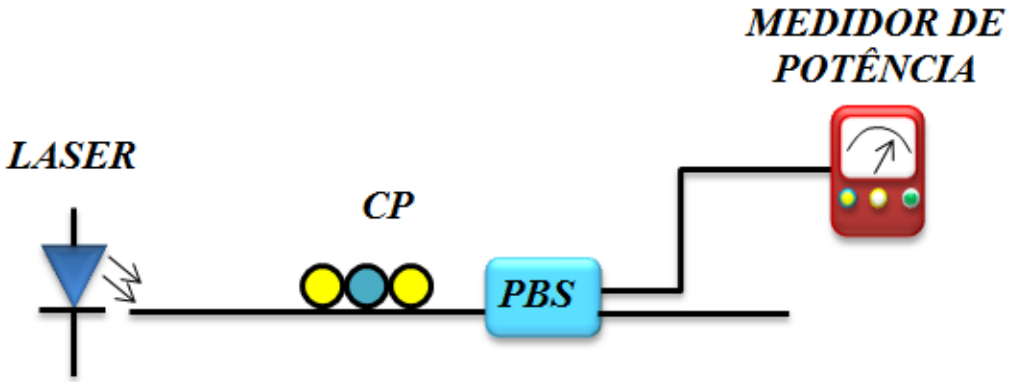


Fonte: elaborada pelo autor.

8 MEDIÇÃO DO DOP CLÁSSICO DA LUZ EMITIDA POR LASER SEMICONDUTOR VIA MEDIÇÃO DA VISIBILIDADE

A medição do grau de polarização quântico requer contadores de fótons. A medição do DOP através do uso de detectores tradicionais acaba por fazer uma média. Uma forma simples de medir o DOP é através da medição da visibilidade do esquema mostrado na FIGURA 26 (NASCIMENTO; RAMOS, 2005).

Figura 26 – Esquema óptico para a medição de visibilidade de polarização.



Fonte: adaptada de Nascimento e Ramos (2005).

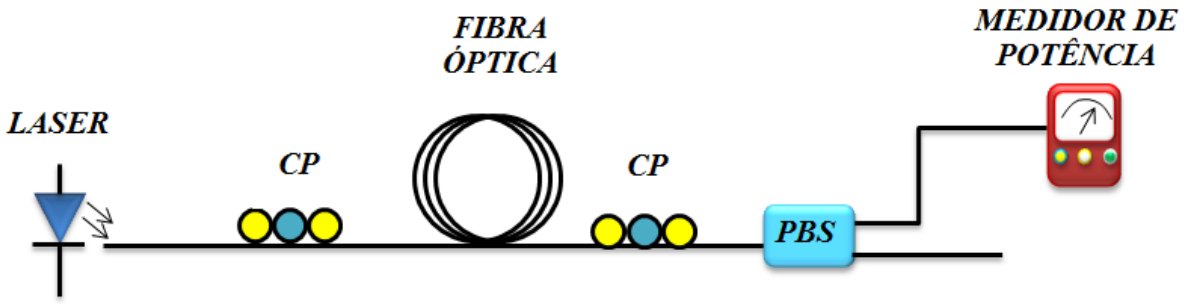
O DOP é calculado como a fração da potência total que é controlada pelo controlador de polarização. Portanto, o DOP pode ser estimado pela visibilidade, que é dada por

$$V = \frac{P_{Máx} - P_{Mín}}{P_{Máx} + P_{Mín}}. \tag{8.1}$$

Em (8.1), P_{max} e P_{min} são, respectivamente, a máxima e a mínima potência medida quando o controlador de polarização é ajustado.

Para medir o quanto um canal despolariza a luz, um trecho de fibra óptica é inserido, como mostrado na FIGURA 27.

Figura 27 – Esquema óptico para medição da visibilidade após a propagação em um trecho de fibra óptica



Fonte: adaptada de Nascimento e Ramos (2005).

8.1 Medição da Visibilidade Usando o Medidor de Potência Óptica

No primeiro experimento realizado a visibilidade foi medida usando o esquema da FIGURA 27, para três valores de corrente do laser (JDS Uniphase, modelo CQF915/408-19330): I_1 = 7 mA (chamado estado térmico pois o laser está operando abaixo do limiar); I_2 = 15 mA (chamado estado joelho pois o laser está operando no joelho da curva corrente versus potência); I_3 = 30 mA (chamado estado coerente pois o laser está operando bem acima do limiar). Para cada estado as medidas foram realizadas ajustando-se o segundo CP para obter o máximo de potência no medidor de potência, feito isso, as medições eram realizadas rotacionando apenas a segunda lente do segundo CP no sentido anti-horário, variando de 0º à 90º com intervalos de 5º, com um total de 19 pontos.

Nas FIGURAS 28, 29 e 30 têm-se os gráfico da Potência Óptica versus Ângulo para os estados Coerente, Joelho e Térmico, respectivamente. Foram utilizados três comprimentos de fibra óptica: a cor azul representa a fibra de 100 m; a cor preta representa a fibra de 500 m; e a cor vermelha representa a fibra de 1000 m.

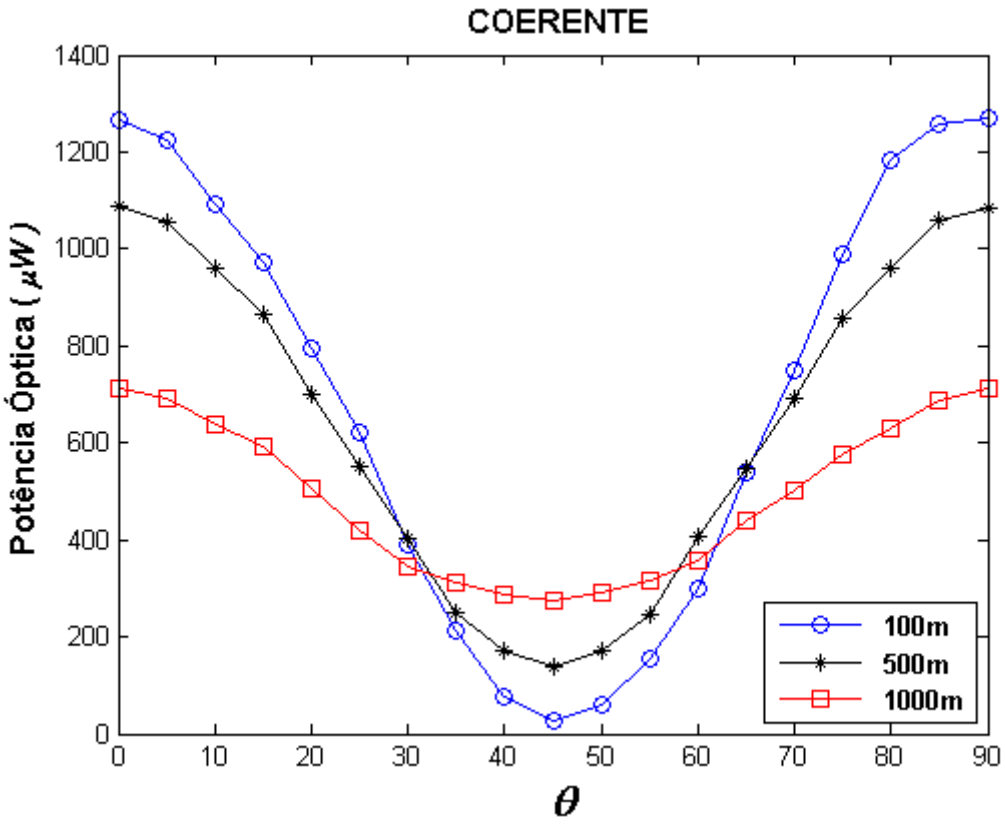
Na TABELA 6 tem-se os valores de visibilidade correspondente a cada estado e para cada comprimento.

Tabela 6 – Visibilidade para os estados Coerente, Joelho e Térmico, para fibras de 100 m, 500 m, e 1000 m.

VISIBILIDADE			
Comprimento (m)	**Coerente**	**Joelho**	**Térmico**
100	0.9596	0.9263	0.8626
500	0.7737	0.6561	0.5827
1000	0.4437	0.4282	0.4090

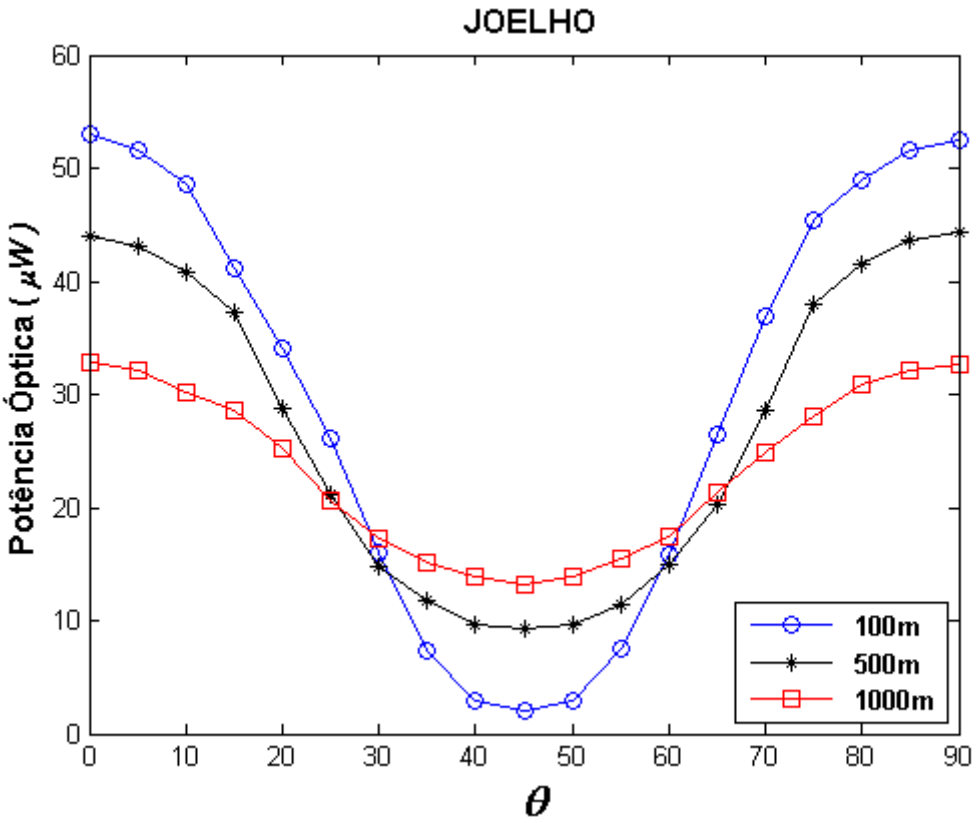
Fonte: elaborada pelo autor.

Figura 28 – Potência óptica versus a rotação do controlador de polarização. Estado Coerente.



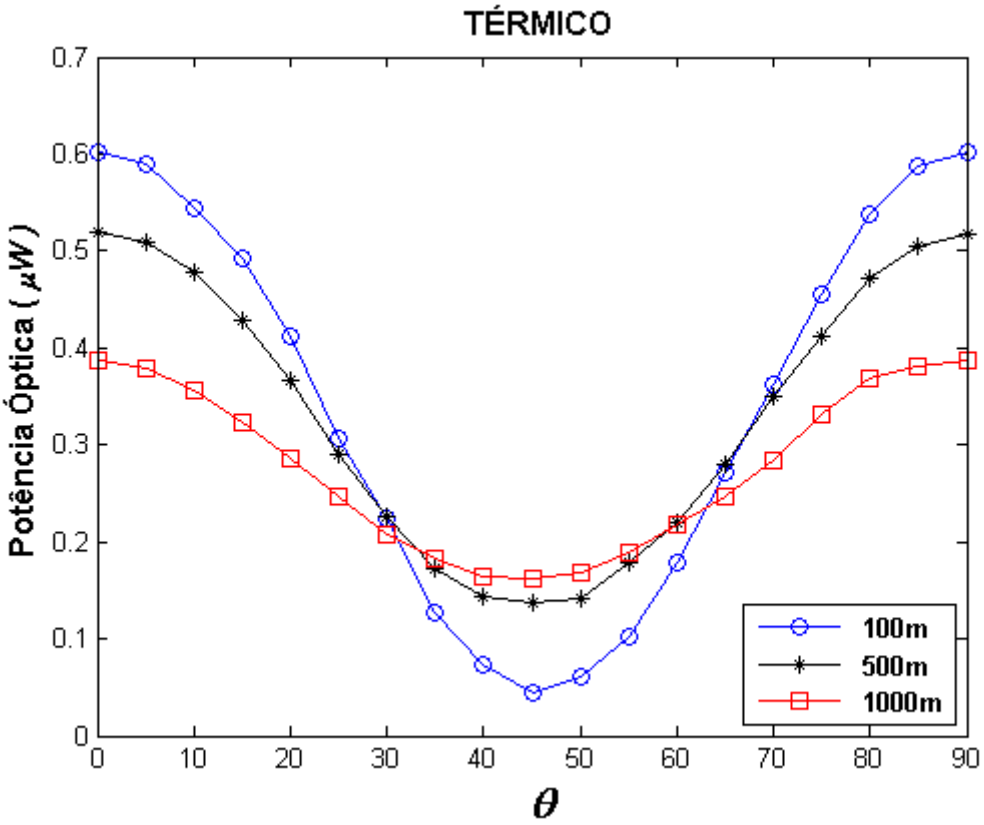
Fonte: elaborada pelo autor.

Figura 29 – Potência óptica versus a rotação do controlador de polarização. Estado Joelho.



Fonte: elaborada pelo autor.

Figura 30 – Potência óptica versus a rotação do controlador de polarização. Estado Térmico.

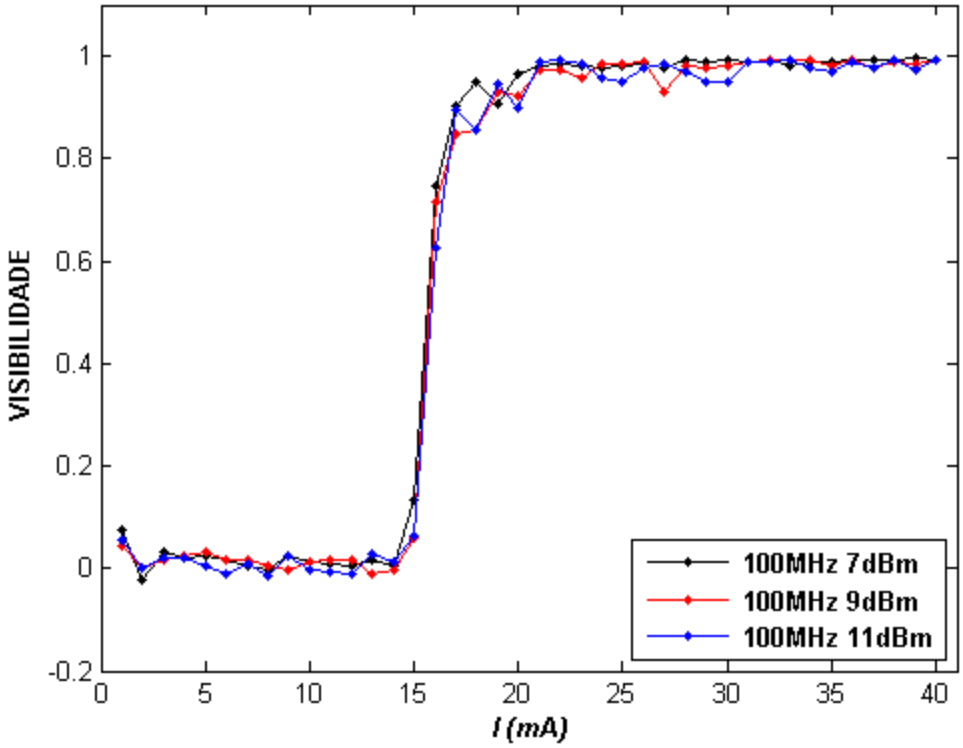


Fonte: elaborada pelo autor.

8.2 Medição da Visibilidade Usando Modulação Externa e o Analisador de Espectro

Uma segunda medição da visibilidade foi realizada, mas agora fazendo uma modulação direta no laser e medindo, com o uso do analisador de espectro, a potência elétrica da raia correspondente à frequência do sinal modulante. Além disso, a corrente de injeção do laser foi variada de na faixa de 0 a 40 mA, com o passo de 1mA. Como o objetivo é verificar a visibilidade como função da corrente do laser, nenhum canal despolarizador foi inserido. O resultado pode ser visto na FIGURA 31, para um sinal modulante de 100 MHz. Nesta figura podem-se perceber três regiões distintas: I) baixa visibilidade na região até aproximadamente 15 mA, quando o laser ainda opera abaixo da corrente de limiar. II) alta visibilidade na região com corrente maior que 20 mA, quando o laser já está operando acima do limiar. III) visibilidade crescente (com alto valor da derivada primeira) na faixa entre 15 mA e 20 mA. Como a modulação utilizada foi de amplitude (modulação da corrente do laser), este comportamento pode ser explicado pela largura espectral do laser nas diferentes regiões citadas. Quanto maior a corrente, menor a largura espectral e maior a visibilidade.

Figura 31 – Visibilidade versus corrente para o sinal de 100 MHz



Fonte: elaborada pelo autor.

9 CONCLUSÕES E PERSPECTIVAS DE TRABALHOS FUTUROS

9.1 Conclusões

A presente tese pode ser dividia em três partes: I) Protocolos de comunicação quântica Segura Direta. II) Detecção homódina de fótons. III) Polarização quântica da luz. As conclusões referentes a cada uma dessas partes são as seguintes:

9.1.1 Protocolos de Comunicação Quântica Segura Direta

Três novos esquemas ópticos para QSDC foram propostos. Estes protocolos utilizam a distribuição espectral das fontes luminosas e o uso de moduladores de fase dependentes da frequência para aumentar a segurança. É importante salientar que essas duas condições são verdadeiras no mundo real e geralmente não são levadas em consideração quando da proposição de novos protocolos quânticos. Adicionalmente, o primeiro esquema óptico executa QSDC e QKD ao mesmo tempo, o segundo protocolo utiliza estados térmicos para aumentar a segurança e o terceiro esquema faz QSDC de um sinal analógico. Os protocolos propostos são seguros contra ataques do tipo intercepta-reenvia, divisão de feixes, contagem de fótons e cavalo de Tróia no qual a espiã envia estados quânticos para uma das partes.

9.1.2 Detecção Homódina de Fótons

Foi realizado um experimento de detecção homódina de fótons. Nesse experimento mostrou-se que o sinal analógico transportado por um estado coerente fortemente atenuado pode ser recuperado por um receptor óptico baseado em PIN, que é mais barato e de fácil manuseio (não requer elevadas voltagens nem resfriamento). A desvantagem da detecção homódina é a mesma encontrada em sistemas de detecção coerente, a necessidade de um oscilador local em fase com a portadora de sinal.

9.1.3 Polarização Quântica da Luz.

Inicialmente foi proposta uma nova medida de grau de polarização baseada na entropia de Shannon. Uma particularidade da medida proposta é que, ao invés de estar atrelada a conceitos puramente matemáticos, como a distância entre duas matrizes densidade, ela está atrelada aos resultados de um experimento de medição dos parâmetros de Stokes. A desvantagem dela é que, por conter a entropia de Shannon em sua formulação fica difícil a realização de cálculos analíticos do grau de polarização, sendo necessário na maioria dos casos o uso de simulações numéricas.

Em seguida, foi realizada a análise do grau de polarização de estados contínuos da luz, bem como um estudo da despolarização causada pela distribuição espectral da mesma. Para o caso de fótons únicos, mostrou-se a despolarização causada por um canal com ruído de fase e para estados coerentes mostrou-se a despolarização devido ao alargamento no domínio da frequência. Em outras palavras, se a energia é distribuída entre mais osciladores, estes terão número médio de fótons pequenos o que diminui o grau de polarização de cada oscilador (frequência) individual.

Por fim, foram realizados dois experimentos para medir o grau de polarização através da medição da visibilidade de polarização. O primeiro experimento mostrou que a visibilidade piora com o comprimento do canal e com a diminuição da corrente de injeção de laser. O segundo experimento comprovou que a visibilidade depende fortemente da corrente de injeção do laser. Os resultados de ambos os experimentos estão de acordo com o que a teoria prevê.

9.2 Perspectivas de Trabalhos Futuros

Como perspectivas de trabalhos futuros pode-se citar:

1) Realização experimental dos protocolos propostos neste trabalho.

2) Aperfeiçoar o experimento de medição homódina de fótons e utilizá-lo na caracterização de fontes de estados quânticos e na realização experimental de protocolos de QKD.

3) Calcular o grau de polarização de outros estados quânticos da luz, bem como analisar a despolarização causada por outros tipos de canais.

REFERÊNCIAS

AGARWAL, G. S.; LEHNER, J.; PAUL, H. Invariances for states of light and their quasi-distributions. **Optics Communications**, v. 129, n. 5-6, p. 369, 1996.

AGARWAL, G. S.; CHATURVEDI, S. Scheme to measure quantum Stokes parameters and their fluctuations and correlations. **Journal of Modern Optics**, v. 50, n. 5, p. 711-716, 2003.

BARRANCO, A. V.; BORELLI, L. F. M. Continuous variable quantum key distribution using polarized coherent states, **International Journal of Modern Physics B**, v. 20, p. 1287, 2006.

BENNETT, C. H.; BRASSARD, G. Quantum cryptography: public key distribution and coin tossing. **Proceedings of IEEE International Conference on Computers Systems and Signal Processing**. Bangalore, India, p. 175 – 179, 1984.

BENNETT, C. H. Quantum cryptography using any two nonorthogonal states. **Physical Review Letters**, v. 68, n. 25, p. 3121 – 3124, 1992.

BERGLUND, A. J. **Quantum coherence and control in one- and two-photon optical systems**. Disponível em: < https://arxiv.org/pdf/quant-ph/0010001.pdf>. Acesso em 13 de abr. 2016.

BRASSARD, G. *et al*. Limitations on Practical Quantum Cryptography. **Physical Review Letters**, v. 85, n. 6, 2000.

BRASSARD, G. **Modern Cryptology: A Tutorial, Lecture Notes in Computer Science**, New York, Springer, v. 325, 1988.

CAVALCANTI, M. D. S.; MENDONÇA, F. A.; RAMOS, R. V. Spectral method for characterization of avalanche photodiode working as single-photon detector. **Optics Letters**, v. 36, n. 17, p. 3446 – 3448, 2011.

CHANG, Y. *et. al*. Quantum secure direct communication and authentication protocol with single photons. **Quantum Information**, v. 58, n. 36, p. 4571 – 4576, 2013.

CHIRKIN, A. S.; ORLOV, A. A.; PARASHCHUK, D. Y. Quantum theory of two-mode interactions in optically anisotropic media with cubic nonlinearities: Generation of quadrature-and polarization-squeezed light. **Quantum Electronics**, v. 23, n. 10, 1993.

DAMASCENO, R. L. C.; **Comunicação quântica segura direta usando distribuição quântica de chaves**. 2017. Dissertação (Mestrado em Engenharia de Telecomunicações) – Instituto Federal de Educação, Ciência e Tecnologia do Ceará, Fortaleza, 2017.

DENG, F. G.; LONG, G. L. Secure direct communication with a quantum one-time pad. **Physical Review A**, v. 69, 2004.

DENG, F. G.; LONG, G. L.; LIU, X. S. Two-step quantum direct communication protocol using the Einstein-Podolsky-Rosen pair block. **Physical Review A**, v. 68, 2003.

DIFFIE, W.; HELLMAN, M. E. New directions in cryptography. **IEEE Transactions on Information Theory**, v. 22, p. 644 – 654, 1976.

EKERT, A. K. Quantum Cryptography Based on Bell's Theorem. **Physical Review Letters**, v. 67, n. 6, p. 661 – 663, 1991.

GAO, F. *et al*. Revisiting the security of quantum dialogue and bidirectional quantum secure direct communication. **Science in China Series G**: Physics, Mechanics & Astronomy, v. 51, n. 5, p. 559 – 566, 2008.

GISIN, N. *et. al.* Quantum cryptography. **Reviews of Modern Physics**, v. 74, 2002.

GONG, Y. X. *et al*. Dependence of the decoherence of polarization states in phase-damping channels on the frequency spectrum envelope of photons. **Physical Review A**, v. 78, n. 4, 2008.

GUERRA, A. G. A. H.; RIOS, F. F. S.; RAMOS, R. V. Quantum secure direct communication of digital and analog signals using continuum coherent states. **Quantum Information Process**, v. 15, p. 4747 – 4758, 2016.

HAUS, H. A. **Electromagnetic Noise and Quantum Optical Measurements**. New York, Springer, 2000.

INOUE, K.; IWAI, Y. Differential-quadrature-phase-shift quantum key distribution. **Physical Review A**, v. 79, 2009.

JONES JÚNIOR, W. B. **Introduction to Optical Fiber Communication Systems**. Oxford University Press, USA, 1995.

KOROLKOVA, N. *et al*. Polarization squeezing and continuous-variable polarization entanglement. **Physical Review A**, v. 65, 2002.

KLIMOV, A. B. *et al*. **Distance-based degrees of polarization for a quantum field**. Disponível em: <https://arxiv.org/pdf/quant-ph/0504226.pdf>. Acesso em 04 de mai. 2016.

LEHNER, J. *et al*. Unpolarized light: Classical and quantum states. **Physical Review A**, v. 53, 1996.

LEONHARDT, U. **Measuring the Quantum State of Light**. Cambridge University Press, v. 1, 1997.

LIU, Z. *et al*. Quantum secure direct communication with optimal quantum superdense coding by using general four-qubit states. **Quantum Information Processing**, v. 12, p. 587 – 599, 2013.

LONG, G. L.; LIU, X. S. Theoretically efficient high-capacity quantum-key-distribution scheme. **Physical Review A**, v. 65, 2002.

LUIS, A. Degree of polarization in quantum optics **PHYSICAL REVIEW A**, v. 66, 2002.

MENDONÇA, F. A. **Análise teórica e resultados experimentais de sistemas de distribuição quântica de chaves usando fótons isolados e estados coerentes mesoscópios**. 2006. Dissertação (Mestrado em Engenharia de Teleinformática) – Centro de Tecnologia, Universidade Federal do Ceará, Fortaleza, 2006.

MENDONÇA, F. A.; DE BRITO, D. B.; RAMOS, R. V. An optical scheme for quantum multi-service network. **Quantum Information and Computation**, v. 12, p. 620, 2012.

NASCIMENTO, J. C.; RAMOS, R. V. Dynamic of the degree of polarization in a depolarizing channel: theory and experimental results. **Microwave and Optical Technology Letters**, v. 47, n. 5, p. 497 – 500, 2005.

NAMEKATA, N. *et al*. Differential phase shift quantum key distribution using single-photon detectors based on a sinusoidally gated InGaAs/InP avalanche photodiode. **Applied Physics Letters**, v. 91, 2007.

PINHEIRO, P. V. P.; RAMOS, R. V. Two-layer quantum key distribution. **Quantum Information Process**, v. 14, n. 6, p. 2111 – 2124, 2015.

PRAKASH, H.; CHANDRA, N. Density Operator of Unpolarized Radiation. **Physical Review A**, v. 4, p. 796, 1971.

RAMOS, R. V. **Contribuições às comunicações quânticas em redes ópticas**. 2000. Tese (Doutorado em Engenharia Elétrica) – Faculdade de Engenharia Elétrica e de Computação, Universidade Estadual de Campinas, Campinas, SP, 2000.

RAMOS, R. V.; SOUZA, R. F. Simulations of continuum coherent states and its use in quantum cryptographic systems. **Jourrnal of Modern Optics**, v. 48, n. 6, p. 989 – 1003, 2001.

RIGOLIN, G.; RIEZNIK, A. A. Introdução à criptografia quântica. **Revista Brasileira de Ensino de Física**, v. 27, n. 4, p. 517 – 526, 2005.

RIOS, F. F. S.; GUERRA, A. G. A. H.; RAMOS, R. V. Quantum Communication with Continuum Single-Photon, Two-photon and Coherent. **Quantum Information & Computation**, v. 17 n. 15-16, p. 1277 – 1291, 2017.

RIVEST, R. L.; SHAMIR, A.; ADLEMAN, L. A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. **Communications of the ACM**, v. 21, n. 2, 120 – 126, 1978.

SANTOS, D. J.; LOUDON, R.; FRAILE-PELÁEZ, F. J. Continuum states and fields in quantum optics. **American Journal of Physics**, v. 65, p. 126, 1997.

SILVA, J. B. R.; RAMOS, R. V. On the quantum polarization and entanglement of superpositions of two two-mode coherent states. **Optics Communications**, v. 281 p. 6034 – 6039, 2008.

SILVA, M. B. C. *et al*. Homodyne detection for quantum key distribution: an alternative to photon counting in BB84 protocol. *In*: PHOTONICS NORTH CONFERENCE PROCEEDING, 6343., 2006, Quebec, Conferência.

SÖDERHOLM, J. *et al*. Unpolarized light in quantum optics. **Optics and Spectroscopy**, v. 91, n. 4, p. 532 – 534, 2001.

STANTON, M. **Segurança na organização governamental**. Disponível em: <http://www.wirelessbrasil.org/michael_stanton/artigos/2000/jun_26.html>. Acesso em 17 abr. 2017.

USACHEV, P. Experimental verification of differences between classical and quantum polarization properties. **Optics Communications**, v. 193, n. 1-6, p. 161 – 173, 2001.

ZBINDEN, H. *et al*. Quantum Cryptography. **Applied Physics B**, v. 67, p. 743 – 748, 1998.