UNIVERSIDADE FEDERAL DO CEARÁ
CENTRO DE TECNOLOGIA
DEPARTAMENTO DE ENGENHARIA DE TELEINFORMÁTICA
PROGRAMA DE PÓS-GRADUAÇÃO EM ENGENHARIA DE TELEINFORMÁTICA

JOSÉ CLÁUDIO DO NASCIMENTO

CORREÇÃO DE ERRO EM SISTEMAS DE COMUNICAÇÃO QUÂNTICA UTILIZANDO POLARIZAÇÃO DE ESTADOS COERENTES E FÓTONS ISOLADOS

FORTALEZA - CE
SETEMBRO DE 2006

UNIVERSIDADE FEDERAL DO CEARÁ
CENTRO DE TECNOLOGIA
DEPARTAMENTO DE ENGENHARIA DE TELEINFORMÁTICA

CORREÇÃO DE ERRO EM SISTEMAS DE COMUNICAÇÃO QUÂNTICA UTILIZANDO POLARIZAÇÃO DE ESTADOS COERENTES E FÓTONS ISOLADOS

Autor
JOSÉ CLÁUDIO DO NASCIMENTO

Orientador
RUBENS VIANA RAMOS

Dissertação submetida à Coordenação do Curso de Pós-graduação em Engenharia de Teleinformática da Universidade Federal do Ceará, como parte dos requisitos exigidos para obtenção do grau de **Mestre em Engenharia de Teleinformática.**

FORTALEZA-CE
SETEMBRO DE 2006

N195c Nascimento, José Claúdio do

Correção de erro em sistemas de comunicação quântica utilizando polarização de estados coerentes e fótons isolados.

6zp.

Dissertação (mestrado) – Universidade Federal do Ceará, Centro de Tecnologia, Departamento de Engenharia de Teleinformática, Fortaleza – CE, 2006.

Orientador: Dr. Rubens Viana Ramos.

1. Teleinformática. 2. Comunicações óticas. 3. Criptografia de dados. I. Título. II Orientador.

CDD 621.38

JOSÉ CLÁUDIO DO NASCIMENTO

CORREÇÃO DE ERRO EM SISTEMAS DE COMUNICAÇÃO QUÂNTICA UTILIZANDO POLARIZAÇÃO DE ESTADOS COERENTES E FÓTONS ISOLADOS

Dissertação submetida à Coordenação do Curso de Pós-Graduação em Engenharia de Teleinformática, da Universidade Federal do Ceará, como requisito parcial para a obtenção do grau de Mestre em Engenharia de Teleinformática.

Aprovada em ___/___/_____

BANCA EXAMINADORA

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

_____
Prof. Dr. Jonas Mikael Alexander Söderholm
Universidade de Nihon - Japão

_____
Prof. Dr. Hilma Helena Macedo de Vasconcelos
Universidade Federal do Ceará- DM/UFC

_____
Prof. Dr. Elvio César Giraudo
Universidade Federal do Ceará – DETI/UFC

Aos meus pais, José Manuel do Nascimento e Cícera Maria Conceição Nascimento, e às minhas irmãs Rejane Aparecida do Nascimento e Maria Lílian do Nascimento.

AGRADECIMENTOS

Sobretudo agradeço a Deus, por me colocar nesta passagem em busca de pequenas verdades, percorrendo até agora um caminho rico em conhecimento e questionamentos que tornaram a minha vida interessante.

Ao professor Dr. Rubens Viana Ramos, por ter me oferecido a oportunidade de estudar em seu grupo de pesquisa, me motivado e orientado no desenvolvimento desta dissertação.

Ao professor Dr. Elvio César Giraudo, pela sua contribuição em uns dos trabalhos desenvolvidos nesta dissertação.

Aos colegas do Grupo de Informação Quântica (GIQ) George André, João Batista, Fábio Alencar, Wellington Alves, David Senna, Carol Timbó, Daniel Brito e Paulo Benício, por me darem a felicidade de discutir os conceitos da mecânica quântica tão úteis à maturidade das idéias aqui desenvolvidas e pelos agradáveis momentos de descontração nas horas de almoço e lanche.

Finalmente, meus agradecimentos a FUNCAP, por ter fornecido a bolsa de estudos para que a pesquisa aqui apresentada fosse realizada.

“Mecânica Quântica: Cálculo com magia negra.”

Albert Einstein

RESUMO

Nesta dissertação é realizado um estudo da polarização da luz e suas aplicações em sistemas de comunicações quânticas. Inicialmente, são apresentadas as ferramentas matemáticas necessárias ao tratamento da polarização da luz de fótons isolados e estados coerentes: matriz coerência, parâmetro de Stokes e grau de polarização. Em seguida é apresentada, através de simulação numérica, a dinâmica do grau de polarização da luz de um fóton durante a propagação em um canal despolarizador. Por fim, o resultado de um experimento usando estados coerentes, objetivando medir o grau de polarização da luz após propagação em um trecho de 200 m de fibra, é apresentado. O experimento é útil para a determinação do parâmetro do modelo de canal despolarizador de qubits. Sendo a polarização da luz uma propriedade facilmente alterada por condições ambientais, são estudados os esquemas ópticos que, dentro de certas restrições, podem corrigir variações aleatórias da polarização da luz durante a propagação na fibra. Tais esquemas são empregados como corretores de erros em sistemas de comunicações quânticas. Baseados em esquemas de correção encontrados na literatura, foram propostos dois novos esquemas, um para a utilização em sistemas que empregam polarização de luz de fótons isolados e outro para sistemas que empregam polarização de estados coerentes bimodais, sendo o primeiro ativo, isto é, requer um protocolo de controle e sincronismo, e o segundo passivo. Por fim, é feita a análise da segurança de um sistema de distribuição quântica de chaves, empregando o esquema proposto de correção de erros, quando o mesmo sofre o ataque de Fuchs-Peres-Brandt. É mostrado que a utilização do esquema de correção de erros proposto favorece a visibilidade da presença de um espião monitorando o canal quântico.

ABSTRACT

In this dissertation, it is realized a study of light polarization and its applications in quantum communications. Initially, the mathematical tools needed for single-photon and coherent states polarization analyses are presented: coherence matrix, Stokes parameters and polarization degree. Following, using numerical simulations, it is presented the variation of the degree of polarization of a single-photon pulse during depolarizing channel propagation. At last, the result of an experiment using coherent states, aiming to measure the degree of polarization after propagation in 200 m optical fiber is presented. The experiment is useful for determination of the parameter of the qubit depolarizing channel model. Since light polarization is easily changed when environment fluctuations are present during fiber propagation, optical schemes able to correct unpredictable polarization changes are studied. Such schemes are employed for error correction in quantum communication systems. Based on already proposed error correction schemes, two new schemes are proposed, one for systems that employs polarization of single-photon light, and other for systems that employs polarization of two-mode coherent states, being the first active, that is, requiring a control and synchronism protocol, while the second is passive. At last, it is realized a security analysis of a quantum key distribution system, employing the proposed error correction scheme, when the same is under Fuch-Peres-Brandt attack. It is shown that using the proposed error correction scheme the presence of an eavesdropper monitoring the quantum channel is more visible.

SUMÁRIO

LISTA DE FIGURAS

LISTA DE ABREVIATURAS

BS – Divisor de feixes ou acoplador óptico (Beam Splitter)

PBS – Divisor de feixes por polarização (Polarization Beamsplitter).

HWP – Rotacionador de polarização de $\pi/2$ (Half-wave plate).

GVD – Dispersão de velocidade de grupo (Group velocity dispersion).

PMD – Dispersão de modos de polarização (polarization mode dispersion).

COD – Codificador.

DEC – Decodificador.

CODEC – Sistema formado por codificador, canal e decodificador.

DQC – Distribuição Quântica de Chaves.

BB84 – Protocolo de DQC proposto por Bennett e Brassard no ano de 1984.

PC – Célula de Pockels (Pockels Cell).

CQF915/108 – Diodo laser que emite luz CW (onda contínua) operando em 1550.91nm.

PM – Medidor de potência óptica (Power Meter).

IP – Interferômetro de Polarização.

INTRODUÇÃO

Na busca pela evolução da tecnologia da informação, cresce o desafio do desenvolvimento de dispositivos e sistemas melhores, oferecendo resposta em um tempo menor, maior confiabilidade, mais recursos em um espaço cada vez menor e novos serviços. Com a intenção de buscar o desenvolvimento da tecnologia em novos limites, nasce o interesse da engenharia pela mecânica quântica. Quando se considera a hipótese de construir sistemas ou dispositivos que operam com poucas partículas (como, por exemplo, fótons e elétrons), devemos estar atentos às propriedades quânticas. Em particular, a polarização da luz é um dos mais simples sistemas físicos capazes de representar um bit quântico (qubit). Por esta razão, os primeiros sistemas de distribuição quântica de chaves foram realizados utilizando polarização de fótons isolados. Tais sistemas atualmente servem apenas para sistemas de distribuição quântica de chaves de curta distância, devido à despolarização provocada pela propagação da luz em fibras ópticas. Entretanto, sistemas de comunicação quântica utilizando polarização de estados coerentes foram recentemente propostos e representam uma alternativa, de melhor desempenho em relação ao alcance e à velocidade de transmissão de bits úteis, aos sistemas utilizando fótons isolados. Por outro lado, o desenvolvimento de computadores quânticos baseados na polarização da luz continua como uma forte linha de pesquisa, uma vez que portas de um qubit são facilmente implementadas e portas CNOT com probabilidade de sucesso de 25% foram propostas. Portanto, a polarização da luz como portadora de informação quântica, seja com fins de comunicação ou computação, é um tema atual e importante para o desenvolvimento da tecnologia quântica da informação. Contudo, a luz está sujeita à variações aleatórias de sua polarização durante a propagação em um meio que não preserve a polarização, o que causa erros no sistemas de comunicação e computação baseados na polarização da luz. Assim, para que seja possível a implementação prática de sistemas de comunicação e computação quânticas confiáveis usando a polarização da luz é necessário o uso de códigos corretores de erro. Tais códigos podem ser construídos utilizando-se estados entrelaçados ou codificação espaço-temporal. Nesta direção, a presente dissertação trata da correção de erros em sistemas de comunicações quânticas utilizando a polarização de estados coerente e fótons isolados, empregando um código espaço-temporal. A dissertação está estruturada da seguinte forma: No Capítulo 1 a polarização de fótons isolados e estados coerentes é revisada. No Capítulo 2, dois sistemas ópticos implementando o código

espaço-temporal para correção de erro são propostos, um para sistemas que utilizam fótons isolados e outro para sistemas que utilizam estados coerentes. No Capítulo 3, é apresentada a análise de segurança, considerando o ataque Fuch-Peres-Brandt, de um sistema de distribuição quântica de chaves empregando fótons isolados e utilizando o código espaço-temporal. Por fim, são apresentadas as conclusões e perspectivas.

CAPÍTULO 1

Polarização de um fóton e do estado coerente bimodal

1.1 Introdução

Aplicações para um fóton polarizado têm sido propostas para sistemas de comunicação quântica. Distribuições quânticas de chaves foram realizadas utilizando polarização de fótons isolados [1-3]. Entretanto, sistemas de comunicação quântica utilizando polarização de estados coerentes foram recentemente propostos e representam uma alternativa, de melhor desempenho em relação [4] ao alcance e à velocidade de transmissão de bits úteis, aos sistemas utilizando fótons isolados. O grau de polarização quântica da luz para estados coerentes tem sido bastante estudado recentemente [5]. Contudo, a luz está sujeita à variações aleatórias de sua polarização durante a propagação em um meio que não preserve a polarização, o que causa erros no sistemas de comunicação e computação baseados na polarização da luz [6].

A polarização é a propriedade que demonstra o caráter vetorial do campo eletromagnético. Ela é de crucial importância em sistemas de comunicação óptica, pois os diversos componentes ópticos possuem perdas e/ou dispersão dependentes da polarização. Neste último caso, por exemplo, a dispersão dos modos de polarização [Apêndice A] limita a taxa de transmissão em redes ópticas [7-9]. Portanto, um completo conhecimento das propriedades da polarização é de grande importância para que se possa aproveitar ao máximo suas potencialidades.

A polarização clássica da luz pode ser caracterizada matematicamente através da matriz coerência J [10]. Os elementos da matriz J são as autocorrelações (na diagonal) e correlações cruzadas (elementos fora da diagonal) das componentes x e y do campo elétrico. Por outro lado, a matriz densidade, ρ, contém toda a informação disponível sobre um determinado estado quântico [11]. Quando o estado quântico em questão é a polarização de um fóton, J e ρ são iguais. Estas semelhanças estimulam a aplicação de conceitos comuns de uma na outra. Por exemplo, as esferas de Poincaré e Bloch se confundem em semelhança de análise. A vantagem disso é que podemos visualizar a interpretação para medidas de distância e grau de polarização.

Neste capítulo, são trabalhados os conceitos de polarização quântica da luz de um fóton e estados coerentes bimodais, para aplicações em comunicações quânticas. O objetivo é identificar como varia a polarização durante a propagação da luz em uma fibra óptica monomodo. O fenômeno que degrada o desempenho de sistemas de comunicações ópticas que utilizam a polarização da luz é a despolarização. Portanto, a fibra óptica é vista como um canal despolarizador. A grandeza que mede o quanto a luz é polarizada é o grau de polarização, g_p. Portanto, será analisada a variação de g_p, numericamente e experimentalmente, para propagação da luz em um trecho de fibra óptica. A simulação numérica é usada para mostrar a dinâmica da perda do grau de polarização durante a propagação da luz na fibra óptica, e um experimento utilizando estado coerente é realizado para medir o grau de polarização da luz antes e após a propagação em um trecho de fibra monomodo. Este experimento permite encontrar o valor do parâmetro do modelo de canal despolarizador utilizado na simulação numérica.

1.2 Geometria da polarização, matriz coerência (J) e matriz densidade (ρ)

Na polarização da luz de um fóton, no lugar de termos uma distribuição de energia sobre os eixos de polarização, teremos a probabilidade de encontrarmos o fóton em um destes eixos, uma vez que um fóton é indivisível. O estado quântico $|\psi\rangle$, representando a polarização de um fóton, pode ser representado pelo vetor de Stokes $\vec{S}$ ou pela matriz densidade ρ. A forma geral desta última é dada por:

$$\rho = \left|\psi(\theta,\delta)\right\rangle\left\langle\psi(\theta,\delta)\right| = \begin{bmatrix} \cos^2\left(\frac{\theta}{2}\right) & \cos\left(\frac{\theta}{2}\right)\mathrm{sen}\left(\frac{\theta}{2}\right)e^{i\delta} \\ \cos\left(\frac{\theta}{2}\right)\mathrm{sen}\left(\frac{\theta}{2}\right)e^{-i\delta} & \mathrm{sen}^2\left(\frac{\theta}{2}\right) \end{bmatrix}. \tag{1.1}$$

Existem dois graus de liberdade (θ,δ) para a rotação de estados completamente polarizados (ou estados puros) sobre a esfera de Poincaré, abrangendo, assim, toda a superfície da esfera. Podemos escrever os operadores quânticos de Stokes [12-14] para apenas um fóton da seguinte maneira;

$$\hat{S}_0 = \left|H\right\rangle\left\langle H\right| + \left|V\right\rangle\left\langle V\right| = \sigma_0 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \tag{1.2}$$

$$\hat{S}_1 = \left|H\right\rangle\left\langle H\right| - \left|V\right\rangle\left\langle V\right| = \sigma_{1(z)} = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \tag{1.3}$$

$$\hat{S}_2 = \left|V\right\rangle\left\langle H\right| + \left|H\right\rangle\left\langle V\right| = \sigma_{2(x)} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \tag{1.4}$$

$$\hat{S}_3 = i\left(\left|V\right\rangle\left\langle H\right| - \left|H\right\rangle\left\langle V\right|\right) = \sigma_{3(y)} = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}. \tag{1.5}$$

Em (1.2)-(1.5) $|H\rangle$ e $|V\rangle$ representam, respectivamente, os estados quânticos de polarização linear horizontal e vertical, e σ_i são as matrizes de Pauli. Os valores médios dos operadores quânticos de Stokes $s_i = \left\langle \hat{S}_i \right\rangle = Tr\left(\rho \hat{S}_i\right) = Tr\left(\rho\sigma_i\right)$, i=1,2,3, formam o vetor de Stokes $[s_0\ s_1\ s_2\ s_3]^T$. A matriz densidade do estado quântico da polarização de um fóton pode ser escrita em função dos elementos do vetor de Stokes:

$$\rho = \frac{1}{2}\begin{bmatrix} 1+s_1 & s_2 - is_3 \\ s_2 + is_3 & 1-s_1 \end{bmatrix} = \frac{1}{2}\sum_{i=0}^{3} s_i\sigma_i\,. \tag{1.6}$$

Usando (1.6) e o fato que $Tr(\sigma_i\sigma_j)=2\delta_{ij}$ em (1.1), obtemos o vetor de Stokes $\vec{S}=[s_0,s_1,s_2,s_3]$ para o estado de polarização (1.1):

$$\vec{S}=\left[1,\cos(\theta),\text{sen}(\theta)\cos(\delta),\text{sen}(\theta)\text{sen}(\delta)\right]. \tag{1.7}$$

Neste trabalho usamos o vetor reduzido de Stokes $\vec{S}'=[s_1,s_2,s_3]$, que é um vetor que aponta da origem da esfera de Poincaré para o ponto de localização do estado de polarização. A partir do vetor reduzido de Stokes podemos fazer uma análise vetorial dos estados quânticos contidos em qualquer lugar sobre a superfície da esfera de Poincaré ou no interior dela. Por fim, é importante ressaltar que, para os estados quânticos que estão sobre a superfície da esfera, representando, portanto estados puros, tem-se $\|\vec{S}'\|=1$ e, para os estados quânticos que estão no interior da esfera, representando, portanto estados mistos, tem-se $\|\vec{S}'\|<1$.

1.3 Despolarização

A polarização do fóton tem sido usada como portadora de informação em comunicações quânticas. Ela tem a vantagem de não ser uma variável dependente das perdas na fibra óptica. Por outro lado, a polarização da luz é dependente de diversos fatores, como as formas e composições do núcleo e casca da fibra óptica, emendas, tensões mecânicas (curvaturas e vibrações) e temperatura. Como resultado, para que o processo de comunicação seja eficiente, um controle rigoroso da polarização deve ser feito, inclusive com o uso de fibras especiais que mantêm a polarização fixa, chamadas fibras PM.

Um efeito fortemente indesejado em comunicações ópticas é a despolarização da luz. Do ponto de vista físico, a despolarização é causada pelo PMD. Cada componente espectral do pulso luminoso evolui, independentemente e aleatoriamente para um estado de polarização em geral diferente. A luz totalmente despolarizada é completamente indistinguível de qualquer outro

estado de polarização, por isso não se presta para portar informação. A matriz densidade da luz totalmente despolarizada ρ_m é $I/2$, sendo I a matriz identidade.

Ao se propagar pela fibra óptica, a luz inicialmente completamente polarizada, com grau de polarização máximo (e entropia mínima), evolui para estados parcialmente polarizados, com grau de polarização intermediário (entropia intermediária), até se tornar totalmente despolarizada, com grau de polarização mínimo (entropia máxima). Portanto, ao longo da propagação, o grau de polarização (entropia) tem dinâmica decrescente (crescente). Uma luz parcialmente polarizada ρ pode ser escrita como uma superposição de um estado maximamente misto $I/2$ com um estado puro ρ_p da seguinte maneira:

$$\begin{aligned}\rho(z) &= \frac{I}{2} + \frac{1}{2}\sum_{i=1}^{3} s_i(z)\sigma_i = [1-\xi(z)]\frac{I}{2} + \xi(z)\left[\frac{I}{2} + \frac{1}{2}\sum_{i=1}^{3}\frac{s_i(z)}{\xi(z)}\sigma_i\right] \\ &= [1-\xi(z)]\frac{I}{2} + \xi(z)\rho_p(z).\end{aligned} \tag{1.8}$$

Assim o grau de polarização do fóton é dado por:

$$\xi(z) = \sqrt{\sum_{i=1}^{3} s_i(z)^2}\ . \tag{1.9}$$

A equação (1.9) define o grau de polarização da luz de um fóton (neste caso, s_0=1). Além disso, como pode ser observado em (1.8), $\sum_{i=1}^{3}\left[s_i(z)/\xi(z)\right]^2 = 1$, o que, por definição, indica que ρ_p é sempre puro. De (1.8)-(1.9), vemos que a despolarização da luz implica em $\xi(z)\to 0$, ou seja, $s_i(z)\to 0$, a medida que a luz se propaga pela fibra óptica. Como os parâmetros de Stokes se tornam nulos depende de como o canal despolariza a luz. No modelo proposto em [15], os parâmetros de Stokes variam da seguinte forma:

$$s_1(z) = s_1(0)e^{-2\gamma z};\ s_2(z) = s_2(0)e^{-\gamma z}\ ;s_3(z) = s_3(0)e^{-\gamma z}. \tag{1.10}$$

Em (1.10), o parâmetro γ indica a "força" com que o canal despolariza a luz. Usando (1.10), pode ser vista na Figura 1.1 a dinâmica do grau de polarização, $\xi(z)$, ao longo da distância percorrida.

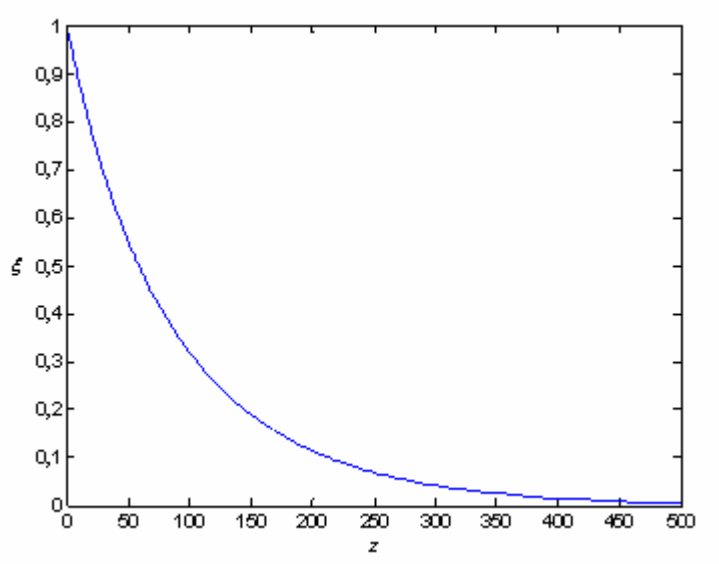

Figura 1.1 – Dinâmica do grau de polarização da luz de um fóton para o canal modelado por (1.10) com γ=0,01, $s_1(0)$=0,530, $s_2(0)$=0,152 e $s_3(0)$=0,86151.

Por outro lado, a Figura 1.2 mostra a evolução dos parâmetros de Stokes da parte completamente polarizada, $s_i'(z) = s_i(z)/\xi(z)$, i=1, 2 e 3.

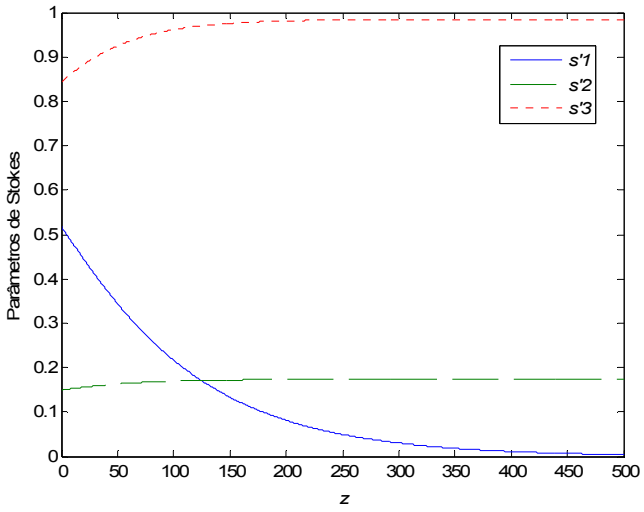

Figura 1.2 – Estabilização dos parâmetros de Stokes da parte pura da polarização da luz de um fóton, para o canal modelado por (1.10), com γ=0,01, $s_1(0)$=0,530, $s_2(0)$=0,152 e $s_3(0)$=0,86151.

Nas simulações mostradas nas Figuras 1.1 e 1.2 os seguintes valores foram usados: γ=0,01, $s_1(0)$=0,530, $s_2(0)$=0,152 e $s_3(0)$=0,86151. Como pode ser observado na Figura 1.2, o estado de polarização da parte completamente polarizada tende monotonicamente para um estado estacionário. Por fim, a Figura 1.3 mostra, para o canal cujo decremento dos parâmetros de Stokes é modelado por (1.10), como um estado no início completamente polarizado e seu par ortogonal, localizados na superfície da esfera de Poincaré, tendem para um estado totalmente despolarizado localizado no centro da esfera.

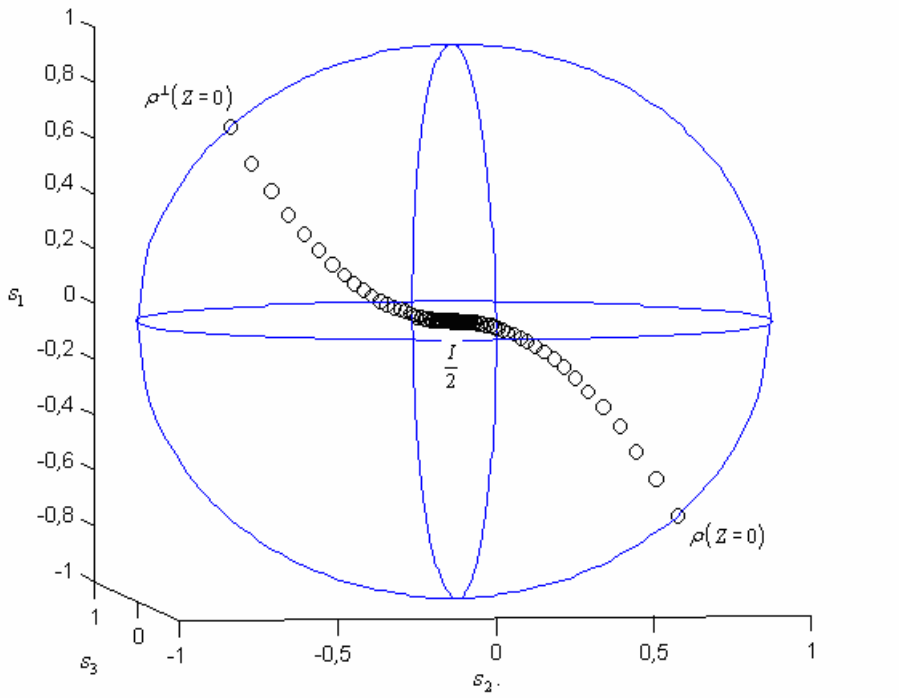

Figura 1.3 – Os estados completamente polarizados $\rho(z=0)$ e seu ortogonal $\rho^{\perp}(z=0)$ caminham para a posição do estado despolarizado $I/2$ que se encontra no centro da esfera.

1.4 Medição de polarização e distinguibilidade

Classicamente, a determinação da polarização de um feixe de luz é obtida pela determinação dos parâmetros de Stokes. Para a luz de um fóton isto não é impossível. Se fosse possível, poderíamos clonar o estado de polarização de um fóton e por abaixo todos os protocolos de distribuição quântica de chaves baseados na polarização de um fóton. Um conceito diretamente ligado à medição da polarização é a capacidade de distinguir dois estados diferentes de polarização. Para a luz de um fóton, dois estados de polarização só são perfeitamente distinguíveis se forem ortogonais. Na Figura 1.4 uma fonte prepara um fóton com polarização descrita pela matriz densidade ρ. Em seguida, este fóton tem sua polarização mensurada por um medidor de polarização (um divisor de feixes por polarização, PBS) que resolve o estado de polarização incidente nos estados ortogonais $|\psi\rangle$ e $|\psi^{\perp}\rangle$.

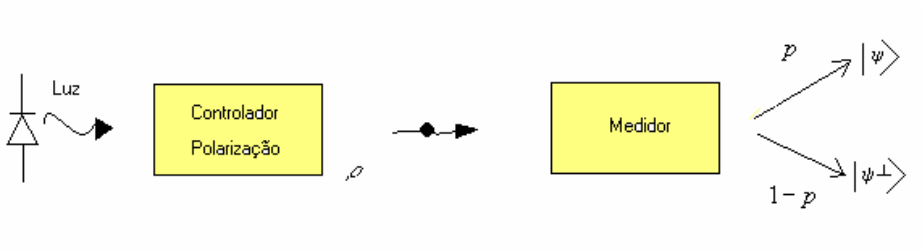

Figura 1.4 – Uma fonte prepara um estado ρ para um medidor que resolve o estado de polarização de entrada na base $|\psi\rangle$ e $|\psi^{\perp}\rangle$.

As probabilidades p e $(1\text{-}p)$ de, após a medição, o fóton emergir com polarização $|\psi\rangle$ e $|\psi^{\perp}\rangle$ são, respectivamente, $p=\langle\psi|\rho|\psi\rangle$ e $(1\text{-}p)=\langle\psi^{\perp}|\rho|\psi^{\perp}\rangle$.

1.5 Polarização de estados coerentes

De forma geral, os operadores quânticos de Stokes são definidos por [12-14]:

$$\hat{S}_0 = \hat{a}_1^{\dagger}\hat{a}_1 + \hat{a}_2^{\dagger}\hat{a}_2, \tag{1.16}$$

$$\hat{S}_1 = \hat{a}_1^{\dagger}\hat{a}_1 - \hat{a}_2^{\dagger}\hat{a}_2, \tag{1.17}$$

$$\hat{S}_2 = \hat{a}_1^{\dagger}\hat{a}_2 + \hat{a}_2^{\dagger}\hat{a}_1, \tag{1.18}$$

$$\hat{S}_3 = -i\left(\hat{a}_1^{\dagger}\hat{a}_2 - \hat{a}_2^{\dagger}\hat{a}_1\right), \tag{1.19}$$

$$\left[\hat{S}_i, \hat{S}_j\right] = 2i\hat{S}_k, \quad \left[\hat{S}_0, \hat{S}_i\right] = 0, \; i = 1,2,3 \quad i,j,k = 1,2,3. \tag{1.20}$$

Em (1.16)-(1.19) $\hat{a}_1^{\dagger}(\hat{a}_1)$ e $\hat{a}_2^{\dagger}(\hat{a}_2)$ são, respectivamente, os operadores de criação (aniquilação) dos modos 1 e 2. A equação (1.20) mostra que, a exceção de $\hat{S}_0$, não é possível determinar simultaneamente, com exatidão, qualquer par de parâmetros quânticos de Stokes. Os valores médios e as variâncias dos parâmetros quânticos de Stokes de um estado coerente $|\alpha,\beta\rangle$ ($|\alpha\rangle$ representa a luz polarizada na direção x e $|\beta\rangle$ a luz polarizada na direção y) são dados por:

$$|\alpha,\beta\rangle = \sum_{n=0}^{\infty} e^{-\frac{|\alpha|^2}{2}} \frac{\alpha^n}{\sqrt{n!}} |n\rangle \otimes \sum_{k=0}^{\infty} e^{-\frac{|\beta|^2}{2}} \frac{\beta^k}{\sqrt{k!}} |k\rangle \tag{1.21}$$

$$\left\langle \hat{S}_1 \right\rangle = |\alpha|^2 - |\beta|^2 \qquad \left\langle \hat{S}_1^2 \right\rangle = \left(|\alpha|^2 - |\beta|^2\right)^2 + |\alpha|^2 + |\beta|^2 \qquad V_1 = |\alpha|^2 + |\beta|^2 \tag{1.22}$$

$$\left\langle \hat{S}_2 \right\rangle = \alpha^*\beta + \alpha\beta^* \qquad \left\langle \hat{S}_2^2 \right\rangle = \left(\alpha^*\beta\right)^2 + \left(\alpha\beta^*\right)^2 + |\alpha|^2 + |\beta|^2 + 2|\alpha|^2|\beta|^2 \qquad V_2 = |\alpha|^2 + |\beta|^2 \tag{1.23}$$

$$\left\langle \hat{S}_3 \right\rangle = i\left(\alpha^*\beta - \alpha\beta^*\right) \qquad \left\langle \hat{S}_3^2 \right\rangle = -\left(\alpha^*\beta\right)^2 - \left(\alpha\beta^*\right)^2 + |\alpha|^2 + |\beta|^2 + 2|\alpha|^2|\beta|^2 \qquad V_3 = |\alpha|^2 + |\beta|^2 \tag{1.24}$$

$$V_i \equiv \left\langle \hat{S}_i^2 \right\rangle - \left\langle \hat{S}_i \right\rangle^2, \quad i = 1,2,3. \quad \left\langle \hat{S}_i \right\rangle = \langle \alpha,\beta | \hat{S}_i | \alpha,\beta \rangle . \tag{1.25}$$

De (1.22)-(1.25) pode-se notar que os parâmetros quânticos exibem flutuações que são expressas por suas variâncias. Para estados coerentes, quanto maior a potência luminosa maior a variância nos três parâmetros. Portanto, em vez de um ponto na esfera de Poincaré, um estado coerente é definido por uma distribuição de probabilidade de estados na superfície da esfera como mostrado na Figura 1.5.

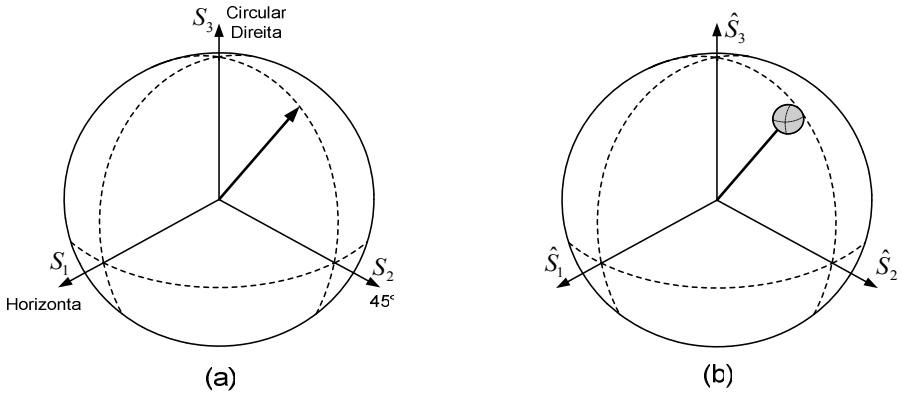

Figura 1.5 – Diagrama dos vetores de Stokes clássico (a) e quântico (b) mapeados na esfera de Poincaré. A bola no final do vetor representa o ruído quântico em $\hat{S}_1$, $\hat{S}_2$ e $\hat{S}_3$.

Para aplicar um deslocamento de fase ϕ entre dois modos linearmente polarizados, é usado o operador unitário [12-14]:

$$U_\phi = \exp\left(i0,5\phi\hat{S}_1\right). \tag{1.26}$$

Por exemplo, quando U_ϕ é aplicado ao estado coerente $|\alpha,\beta\rangle$, o resultado é $\left|\alpha e^{i\phi/2}, \beta e^{-i\phi/2}\right\rangle$. Por outro lado, para uma rotação geométrica de θ na polarização, utiliza-se o operador:

$$U_\theta = \exp\left(i\theta \hat{S}_3\right). \tag{1.27}$$

Assim, uma rotação de θ na polarização do estado coerente $|\alpha,0\rangle$ é obtida fazendo-se $U_\theta|\alpha,0\rangle$, que resulta em $\left|\alpha\cos\theta, \alpha\sin\theta\right\rangle$. No apêndice B está apresentado o desenvolvimento do cálculo para um estado de polarização qualquer na entrada do operador de rotação.

Classicamente, um pulso de luz é despolarizado se seus parâmetros de Stokes são nulos. No entanto, do ponto de vista quântico, esta condição é necessária, mas não suficiente. Um feixe de luz pode ser considerado despolarizado se suas propriedades de observável permanecem inalteradas depois da aplicação de uma rotação geométrica e/ou deslocamento de fase entre suas componentes ortogonais [16]. Esta condição é descrita matematicamente por:

$$\left[\rho, \hat{S}_3\right] = \left[\rho, \hat{S}_1\right] = 0. \tag{1.28}$$

Em (1.28), ρ é a matriz densidade do estado quântico da luz. A forma mais geral de um estado despolarizado é dada por [17,18]:

$$\rho = \sum_n p_n \frac{1}{n+1} \sum_k^n \left|n-k\right\rangle\left|k\right\rangle\left\langle k\right|\left\langle n-k\right|. \tag{1.29}$$

Sendo p_n a função de distribuição de probabilidade do número de fótons considerando ambos os modos.

1.6 Medição experimental do grau de polarização de uma luz CW se propagando por um trecho de fibra

Para medir o grau de polarização de uma luz coerente, usamos o experimento ilustrado na Figura 1.6 [19].

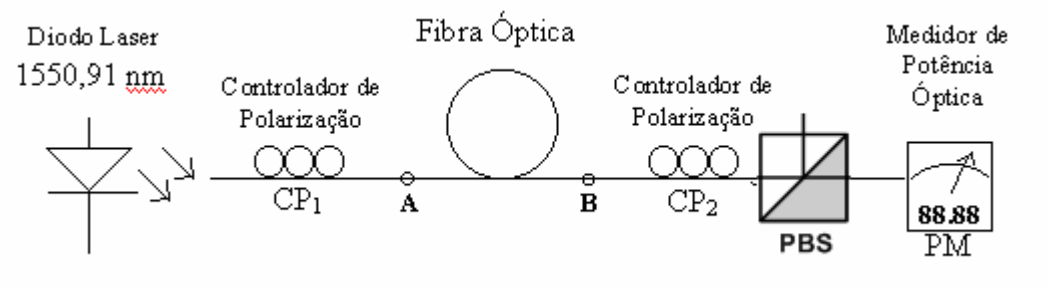

Figura 1. 6 – Experimento para a medição do grau de polarização da luz.

A fonte de luz usada é um diodo laser CQF915/108 que emite um estado coerente CW (onda contínua) operando em 1550,91 nm. O controlador de polarização CP_1 define o estado de polarização a ser usado. O estado escolhido é aquele que maximiza a potência óptica medida na saída inferior do PBS quando o enlace de fibra e o controlador de polarização CP_2 estão ausentes. Em seguida, sem a fibra de teste entre os pontos A e B, os compensadores do CP_2 são ajustados de forma a permitir que a máxima potência óptica seja medida, pelo medidor PM (Power Meter). Neste momento o experimento está calibrado. A primeira medição consiste em, na ausência da fibra entre os pontos A e B, variar o rotacionador de CP_2 e, para cada valor deste, medir a potência óptica. O resultado da observação está ilustrado na Figura 1.7. O grau de polarização para este experimento é dado por:

$$g_p = \frac{P_{\max} - P_{\min}}{P_{\max} + P_{\min}}. \tag{1.30}$$

Em (1.30), P_{max} e P_{min} são, respectivamente, os valores máximo e mínimo encontrado na Figura 1.7.

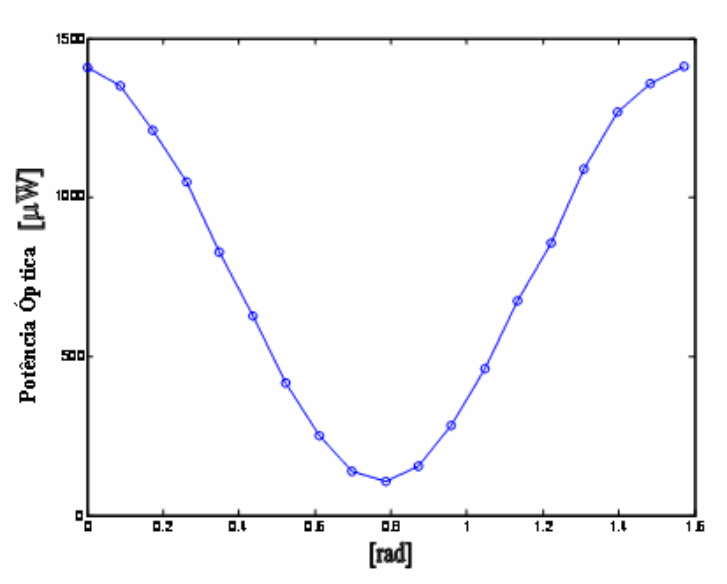

Figura 1. 7 – Variação da potência óptica no experimento da Figura 1.6 sem a fibra de teste.

O valor para o grau de polarização encontrado foi de g_p=0,859. Agora, realiza-se o mesmo procedimento mas com um rolo de fibra de 200m (100m+50m+50m) inserido entre os pontos A e B. O resultado está ilustrado na Figura 1.8.

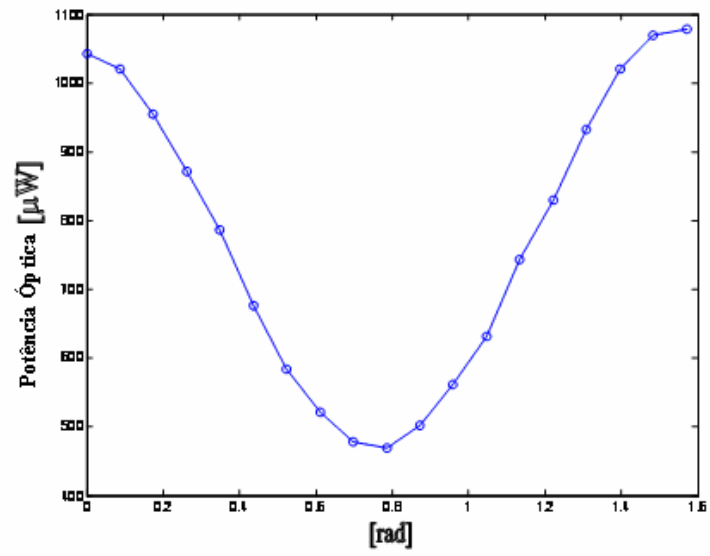

Figura 1.8 – Variação da potência óptica no experimento da Figura 1.6 com a fibra de teste (200m de fibra óptica bobinada).

Comparando-se os gráficos das Figuras 1.7 e 1.8, pode-se observar claramente o efeito do decréscimo do grau de polarização na distinção entre os valores máximo e mínimo de potência óptica medidos. No experimento da Figura 1.8 o grau de polarização obtido foi de g_p=0,394. Assumindo para a fibra óptica o modelo de canal despolarizador [6] expresso por

$$(1-p)\frac{I}{2}+p\rho_e\,, \tag{1.31}$$

sendo ρ_e o estado na entrada da fibra e p a probabilidade do estado de entrada não ser alterado, teríamos, para a fibra testada, p=g_p=0,394.

Embora os resultados tenham sidos obtidos usando luz coerente brilhante (muitos fótons), eles podem ser considerados válidos para luz de fótons isolados pois, como mostrado anteriormente, a polarização da luz de um fóton e da luz coerente são descritos pelo mesmo modelo matemático (matriz coerência igual à matriz densidade). Para o estado coerente a intensidade da luz está distribuída nos modos de polarização expressos na diagonal da matriz coerência. Por outro lado, sabendo que um quantum de luz é indivisível, para a luz de um fóton os elementos da diagonal da matriz coerência representam as probabilidades de encontrarmos o fóton em um dos modos ortogonais. Por isso, os percentuais de energia dos modos de polarização observados no experimento clássico podem expressar probabilidades de encontrarmos o fóton em um dos modos ortogonais no modelo quântico. Então usando um aparato físico para resolver a polarização que vai se tornando indefinida com o aumento do comprimento do canal, concluímos que podemos medir o quanto o canal pode despolarizar a luz.

CAPÍTULO 2

Configurações ópticas para correção de erro em sistemas de comunicações quânticas utilizando polarização de fótons isolados e estados coerentes

2.1 Introdução

Os primeiros sistemas de comunicação quântica experimentais utilizaram polarização de fótons [20-23]. Posteriormente, estes sistemas foram trocados pelos sistemas de comunicação quântica interferométricos [24-29] exatamente devido ao problema da estabilidade da polarização na propagação da luz em longas distâncias. Entretanto, qubits de polarização continuam sendo de grande interesse por três razões: 1) Sistemas de comunicação quântica de curta ou média distância podem ser implementados [30-32]. 2) São bastante utilizados em computação quântica [33-36], 3) Estados entrelaçados, fundamentais para protocolos de comunicação e computação quântica, são experimentalmente mais fáceis de serem produzidos através da criação de pares de fótons com polarização entrelaçada [37-39]. Uma vez produzidos, os fótons do par precisam ser enviados aos usuários da rede óptica de comunicação que desejam realizar um protocolo de comunicação quântica e podem estar distantes de onde os fótons foram gerados.A existência de sistemas de detecção e correção de erros quânticos é fundamental para o desenvolvimento de aplicações de comunicação quântica para longas distâncias em sistemas reais, ou seja, em canais ruidosos variantes no tempo. Muitas das teorias de detecção e correção de erros já apresentadas

[6] são baseadas na introdução de redundância através do uso de múltiplos qubits entrelaçados. Basicamente, um simples qubit é codificado em um estado de vários qubits entrelaçados. Estes códigos têm como objetivo recuperar a informação correta após a passagem da mesma por um canal ruidoso, depois que o erro é detectado através da redundância inserida. Como exemplos, podem ser citados os códigos de Shor [40] e a família de códigos estabelecidos no limite quântico de Hamming para corrigir erros do tipo bit-flip [41].

Em contraste com os modelos construídos com o uso de entrelaçamento, foram propostos em [42] esquemas para a rejeição e correção de erro quântico sem a necessidade de codificação em estados de múltiplos qubits entrelaçados e usando apenas dispositivos de óptica linear. A idéia deste sistema de rejeição e correção de erros quânticos é transformar o qubit de polarização da luz em um qubit do tipo *time-bin* [43], com separação temporal pequena o suficiente para que ambas as componente do qubit se propaguem pela fibra "vendo" o mesmo canal. Por fim, o sistema corretor de erro quântico com óptica linear proposto em [42] não faz uso de redundância para preservar a informação durante a propagação da luz em uma fibra. Neste capítulo, inicialmente é feita uma revisão do sistema de correção de erro proposto em [42] e, em seguida, são apresentadas simplificações dos mesmos e uma extensão para a correção de erros em sistemas de comunicação quântica que utilizam estados coerentes.

2.2 Sistema corretor de erro quântico para comunicação quântica utilizando polarização de fótons isolados

Para a correção de um erro quântico qualquer em um qubit de polarização, foi proposto em [42] a arquitetura mostrada na Figura 2.1.

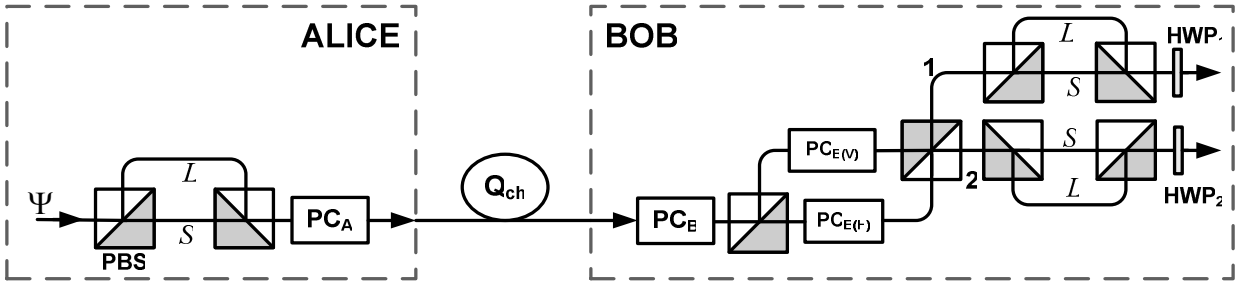

Figura 2.1 – Esquema de correção de erro quântico proposto na referência [42].

Inicialmente, o estado quântico de polarização da luz entrando no sistema óptico é:

$$|\Psi\rangle = a|H\rangle + b|V\rangle . \tag{2.1}$$

Ou seja, o qubit de entrada possui a forma mais geral possível, com $|H\rangle$ e $|V\rangle$ representando, respectivamente, as polarizações horizontal e vertical; e a e b são números complexos que obedecem à condição de normalização $|a|^2+|b|^2=1$. Após a passagem pelo primeiro PBS, a parte horizontal viaja pelo caminho curto (S) enquanto que a parte vertical viaja pelo caminho longo (L). Estes dois pulsos chegarão ao segundo PBS em momentos diferentes e serão guiados para a mesma saída. Neste ponto, "há" dois pulsos separados no tempo de $\Delta t=(l_L-l_S)/V_g$, sendo l_L o comprimento do braço longo, l_S o comprimento do braço curto e V_g a velocidade de grupo, assumida ser a mesma para ambas as polarizações. Assim, o estado quântico logo na saída do interferômetro de polarização (IP) é representado por:

$$|\Psi'\rangle = a|H\rangle_S + b|V\rangle_L . \tag{2.2}$$

A célula de Pockels (PC) situada na saída do IP é acionada de forma a rotacionar de $\pi/2$ somente a polarização do pulso atrasado, assim, o estado na saída do codificador (COD) situado no transmissor (Alice), formado por IP+PC_A, é:

$$\left|\Phi\right\rangle = a\left|H\right\rangle_S + b\left|H\right\rangle_L . \tag{2.3}$$

Devido à existência de variações aleatórias da birrefringência da fibra óptica, o estado na entrada da fibra evolui para um estado desconhecido na saída da fibra. Esta evolução é modelada por uma transformação unitária desconhecida U_f. A forma mais geral de U é dada por:

$$U_f = \begin{bmatrix} \cos(\varphi)\mathrm{e}^{-i\xi} & -sen(\varphi)\mathrm{e}^{i\phi} \\ sen(\varphi)\mathrm{e}^{-i\phi} & \cos(\varphi)\mathrm{e}^{i\xi} \end{bmatrix}. \tag{2.4}$$

Portanto, após a propagação do estado (2.3) pela fibra óptica, o estado na saída desta é:

$$\left|\Phi_f\right\rangle = U_f\left|\Phi\right\rangle = aU_f\left|H\right\rangle_S + bU_f\left|H\right\rangle_L = \tag{2.5}$$

$$\left|\Phi_f\right\rangle = a\left[\cos(\varphi)e^{-i\xi}\left|H\right\rangle_S + sen(\varphi)e^{-i\phi}\left|V\right\rangle_S\right] + b\left[\cos(\varphi)e^{-i\xi}\left|H\right\rangle_L + sen(\varphi)e^{-i\phi}\left|V\right\rangle_L\right] \tag{2.6}$$

$$\left|\Phi_f\right\rangle = a\left[\cos(\varphi)\left|H\right\rangle_S + sen(\varphi)e^{i\lambda}\left|V\right\rangle_S\right] + b\left[\cos(\varphi)\left|H\right\rangle_L + sen(\varphi)e^{i\lambda}\left|V\right\rangle_L\right] \tag{2.7}$$

$$\lambda = \xi - \phi \tag{2.8}$$

A célula de Pockels PC_B na entrada do receptor (Bob) é acionada de forma a rotacionar de $\pi/2$ somente sobre as componentes que percorreram o caminho *S* em Alice. Assim, após PC_B o estado é:

$$\left|\Phi'_f\right\rangle = a\left[\cos(\varphi)\left|V\right\rangle_S + sen(\varphi)e^{i\lambda}\left|H\right\rangle_S\right] + b\left[\cos(\varphi)\left|H\right\rangle_L + sen(\varphi)e^{i\lambda}\left|V\right\rangle_L\right]. \tag{2.9}$$

A equação (2.9) é a entrada do primeiro IP de Bob. Este possui dois braços de igual comprimento e em cada um deles há uma célula de Pockels, $PC_{B(H)}$ (pois são as componentes horizontais de

(2.9) que são a ela encaminhadas) e $PC_{B(V)}$ (pois são as componentes verticais de (2.9) que são a ela encaminhadas). A célula $PC_{B(H)}$ é ativada somente quando está presente a componente do estado que percorreu o caminho *S* em Alice e, a célula $PC_{B(V)}$ é ativada somente quando está presente a componente que percorreu o caminho *L* em Alice. Assim, o estado quântico na saída do primeiro IP de Bob é:

$$\left|\Phi''_f\right\rangle = a\left[\cos(\varphi)\left|V\right\rangle_S^1 + sen(\varphi)e^{i\lambda}\left|V\right\rangle_S^2\right] + b\left[\cos(\varphi)\left|H\right\rangle_L^1 + sen(\varphi)e^{i\lambda}\left|H\right\rangle_L^2\right]. \qquad (2.10)$$

Em (2.10), os índices 1 e 2 significam as duas possíveis saídas do segundo PBS de Bob. Este PBS 2x2 (quatro portas) guia as polarizações horizontal e vertical como mostrado na Figura 2.2.

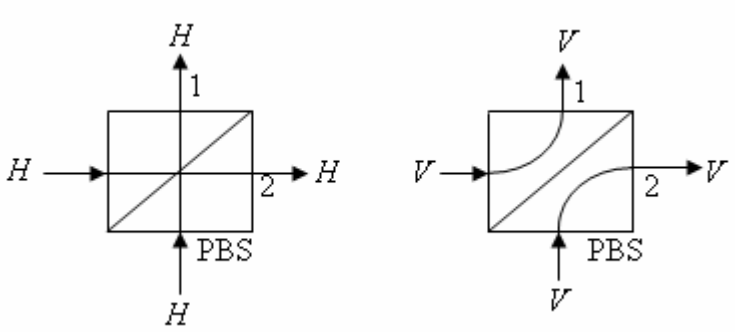

Figura 2.2 – Guiamento dos estados horizontal e vertical de polarização através do PBS 2x2.

Os estados nas saídas 1 e 2 do segundo PBS de Bob passam, cada um deles, por um IP idêntico ao de Alice. A função deles é fazer o balanceamento do tempo de chegada das componentes. Portanto, as saídas dos últimos IPs são;

$$\left|\Phi'''_f\right\rangle = a\left[\cos(\varphi)\left|V\right\rangle_{SL}^1 + sen(\varphi)e^{i\lambda}\left|V\right\rangle_{SL}^2\right] + b\left[\cos(\varphi)\left|H\right\rangle_{LS}^1 + sen(\varphi)e^{i\lambda}\left|H\right\rangle_{LS}^2\right], \qquad (2.11)$$

$$\left|\Phi'''_f\right\rangle = \left[a\cos(\varphi)\left|V\right\rangle_{SL}^1 + b\cos(\varphi)\left|H\right\rangle_{LS}^1\right] + \left[asen(\varphi)e^{i\lambda}\left|V\right\rangle_{SL}^2 + bsen(\varphi)e^{i\lambda}\left|H\right\rangle_{LS}^2\right]. \qquad (2.12)$$

Por fim, na saída de cada IP existe uma placa de meia onda, HWP_1 e HWP_2, que rotaciona de $\pi/2$ a polarização de todas as componentes. Portanto, o estado final nas saídas da configuração óptica apresentada na Figura 2.1 é:

$$\left|\Psi_f\right\rangle = \cos(\varphi)\left(a\left|H\right\rangle + b\left|V\right\rangle\right)^1 + sen(\varphi)e^{i\lambda}\left(a\left|H\right\rangle + b\left|V\right\rangle\right)^2. \tag{2.13}$$

Em (2.13) os sub-índices *SL* e *LS* foram desconsiderados uma vez que significam o mesmo comprimento total. Da equação (2.13) observamos que o estado obtido na saída é o mesmo estado enviado por Alice na entrada. Entretanto, não é possível saber se o qubit está na saída 1 ou na saída 2. O qubit é obtido na saída 1 com probabilidade $\cos^2(\varphi)$ e na saída 2 com probabilidade $\text{sen}^2(\varphi)$. Se o canal é ideal, então φ=0 e o qubit é sempre obtido na saída 1.

Com o objetivo de obter o mesmo resultado com um aparato óptico mais simples, propomos o esquema óptico ilustrado na Figura 2.3.

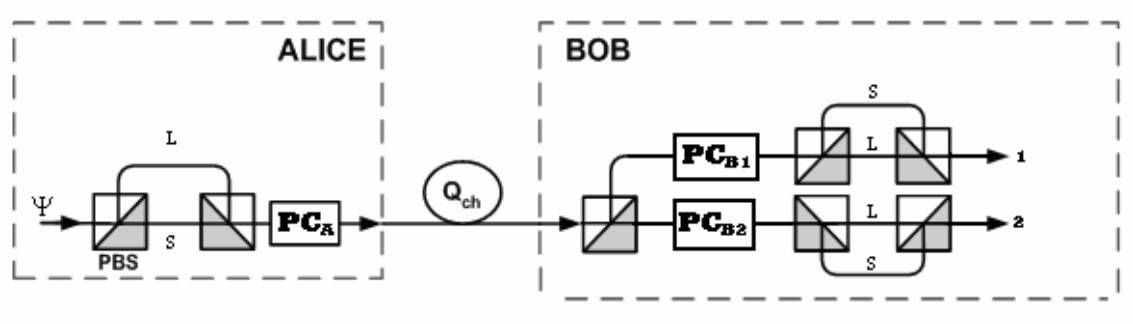

Figura 2.3 – Esquema simplificado do sistema de correção de erro usando óptica linear.

Como pode ser observada, comparando-se os esquemas das Figuras 2.1 e 2.3, a simplificação é feita apenas o decodificador de Bob. Neste, foram retirados a célula PC_B, um PBS e as duas placas de meia onda HWP_1 e HWP_2. A descrição da operação da configuração mostrada na Figura 2.3 começa assumindo que o estado que chega a Bob é aquele dado em (2.7). Logo após o primeiro PBS de Bob, o estado é;

$$\left|\Phi''\right\rangle = a\left[\cos(\varphi)\left|H\right\rangle_S^2 + sen(\varphi)e^{i\lambda}\left|V\right\rangle_S^1\right] + b\left[\cos(\varphi)\left|H\right\rangle_L^2 + sen(\varphi)e^{i\lambda}\left|V\right\rangle_L^1\right], \quad (2.14)$$

$$\left|\Phi''\right\rangle = \cos(\varphi)\left(a\left|H\right\rangle_S^2 + b\left|H\right\rangle_L^2\right) + sen(\varphi)e^{i\lambda}\left(a\left|V\right\rangle_S^1 + b\left|V\right\rangle_L^1\right). \quad (2.15)$$

A célula de Pockels PC_{B1} é acionada de forma a rotacionar de $\pi/2$ o pulso no tempo adiantado (*S*), a célula PC_{B2} é acionada de forma a rotacionar de $\pi/2$ a polarização do pulso no tempo atrasado (*L*). Depois da ação das células de Pockels, o estado total é:

$$\left|\Phi'''\right\rangle = \cos\varphi\left(a\left|H\right\rangle_S^2 + b\left|V\right\rangle_L^2\right) + sen\varphi e^{i\lambda}\left(a\left|H\right\rangle_S^1 + b\left|V\right\rangle_L^1\right). \quad (2.16)$$

Cada estado de (2.16) passa agora por um IP com o mesmo desbalanceamento no comprimento dos braços que o IP de Alice. Entretanto, diferentemente do que ocorre em Alice, a componente vertical viaja pelo braço curto enquanto que a componente horizontal viaja pelo braço longo. Assim, o estado total final após os IPs de Bob é;

$$\left|\Psi_f\right\rangle = \cos(\varphi)\left(a\left|H\right\rangle_{SL}^2 + b\left|V\right\rangle_{LS}^2\right) + sen(\varphi)e^{i\lambda}\left(a\left|H\right\rangle_{SL}^1 + b\left|V\right\rangle_{LS}^1\right), \quad (2.17)$$

$$\left|\Psi_f\right\rangle = \cos(\varphi)\left(a\left|H\right\rangle + b\left|V\right\rangle\right)^2 + sen(\varphi)e^{i\lambda}\left(a\left|H\right\rangle + b\left|V\right\rangle\right)^1. \quad (2.18)$$

Como (2.18) tem significado idêntico a (2.13), concluímos que a variação do esquema da referência [42] apresentada na Figura 2.3 é vantajosa. Além de apresentar redução no número de componentes, o fato de haver uma célula de Pockels a menos facilita a sincronização entre o transmissor e o receptor.

2.3 Sistema corretor de erro quântico para comunicação quântica utilizando polarização de estados coerentes

A utilização de estados coerentes em comunicações quânticas foi recentemente proposta em [44,45]. A vantagem deste sistema em relação aos que utilizam fótons isolados está na velocidade de transmissão e máxima distância entre usuários. Entretanto, atualmente não há certeza se tais sistemas são tão seguros quanto os que utilizam fótons isolados.

Pode ser verificado que os sistemas ópticos apresentados na Seção 2.2 utilizando as células de Pockels também funcionam corretamente quando estados coerentes são utilizados [46]. Entretanto, quando da utilização de estados coerentes, sistemas ópticos passivos de correção de erros podem ser construídos, eliminando a árdua tarefa de sincronização das células de Pockels requerida pelos sistemas da Seção 2.2. O preço a ser pago, como será mostrado, é uma perda da potência óptica útil. O sistema óptico proposto para correção passiva de erros em sistemas que utilizam estados coerentes está ilustrado na Figura 2.4.

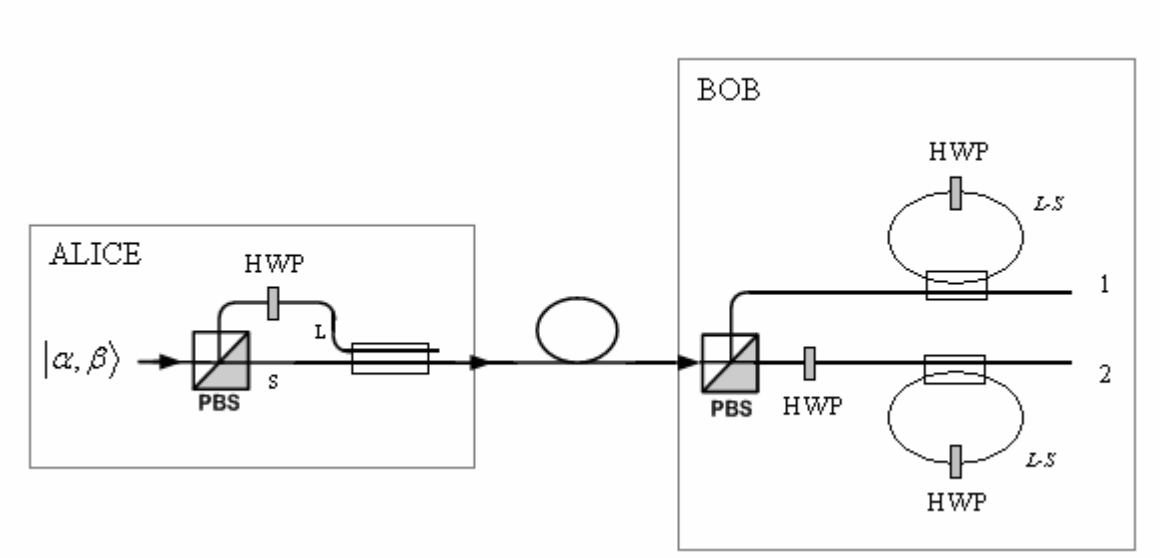

Figura 2.4 – Esquema I do sistema de correção de erro usando dispositivos ópticos passivos para comunicação quântica com estados coerentes.

Como pode ser visto na Figura 2.4, inicialmente o estado de polarização gerado por Alice, $|\alpha,\beta\rangle$, passa por um PBS que separa o pulso óptico incidente em dois pulsos com polarizações

ortogonais, $|\alpha,0\rangle$ (horizontal) e $|0,\beta\rangle$ (vertical). O pulso horizontal é guiado para o caminho curto *S*, enquanto que o pulso vertical é guiado para o caminho longo *L* e tem sua polarização rotacionada de $\pi/2$ pela placa de meia onda HWP, tornando-se $|\beta,0\rangle$. Imediatamente antes do acoplador óptico, os dois pulsos formam o estado quântico $|\alpha,0\rangle_S \otimes |\beta,0\rangle_L$. Ambos os pulsos são inseridos no enlace de fibra através do acoplador óptico (sem perdas) com transmitância *t* e refletância *ir*. Assim, o estado que entra no enlace de fibra é $|ir\alpha,0\rangle_S \otimes |t\beta,0\rangle_L$. Semelhantemente aos sistemas da Seção 2.2, os dois pulsos estão suficientemente próximos de forma a "verem" o mesmo canal óptico. Este é mais uma vez modelado pela evolução unitária dada em (2.4). O resultado da ação do canal óptico nos pulsos enviados por Alice é:

$$\left|ir\alpha\cos(\varphi), ir\alpha sen(\varphi)e^{i\lambda}\right\rangle_S \otimes \left|t\beta\cos(\varphi), t\beta sen(\varphi)e^{i\lambda}\right\rangle_L . \qquad (2.19)$$

A equação (2.19) é, portanto, o estado quântico que chega em Bob. Este estado passa por um PBS que separa as componentes de polarização por dois caminhos (1 e 2) sendo que o caminho inferior possui ainda uma placa de meia onda. Desta forma, o estado quântico total antes dos anéis de fibra é:

$$\left|\Phi\right\rangle = \left|0, ir\alpha sen(\varphi)e^{i\lambda}\right\rangle_S^1 \otimes \left|0, t\beta sen(\varphi)e^{i\lambda}\right\rangle_L^1 \otimes \left|0, ir\alpha\cos(\varphi)\right\rangle_S^2 \otimes \left|0, t\beta\cos(\varphi)\right\rangle_L^2 . \quad (2.20)$$

Por fim, os estados nas saídas 1 e 2 passam, cada um, por um anel de fibra com uma placa de meia onda inserida na realimentação. Os comprimentos dos anéis são iguais ao comprimento *L*-*S* em Alice, e os acopladores ópticos possuem transmitância *T* e refletância *iR*. Assim, quando os pulsos (2.20) passam pelos anéis, uma parte é transmitida e sai do corretor, outra parte é re-inserida no anel. Portanto, na saída de cada anel existe uma seqüência de pulsos, sendo $\left|0, -Rr\alpha sen(\varphi)e^{i\lambda}\right\rangle_s^1 \otimes \left|0, -Rr\alpha\cos(\varphi)e^{i\lambda}\right\rangle_s^2$ os primeiros pulsos a emergirem pelas saídas 1 e 2, respectivamente. O segundo pulso em cada saída é dado por:

$$\left|iT^2r\alpha sen(\varphi)e^{i\lambda}, iRt\beta sen(\varphi)e^{i\lambda}\right\rangle^1 \otimes \left|iT^2r\alpha\cos(\varphi), iRt\beta\cos(\varphi)\right\rangle^2. \quad (2.21)$$

Observando (2.21) pode-se notar que se $T^2r=Rt$ então a polarização do segundo pulso a emergir do sistema corretor, em ambas as saídas, é a mesma do pulso enviado por Alice. Portanto, o sistema óptico da Figura 2.4 efetivamente corrige uma variação desconhecida da polarização. Usando $T^2+R^2=t^2+r^2=1$, na condição $T^2r=Rt$, encontra-se que:

$$\left|T^2r\right|^2 = \frac{X^2(1-X)}{X^2-X+1}. \quad (2.22)$$

Em que $T=\sqrt{X}$. Para encontrar o valor de X que maximiza a potência óptica no segundo pulso a emergir do corretor, deve-se encontrar o valor X de que faça $d(T^2r)/dX=0$. Calculando a derivada de (2.22) em relação a variável X e igualando a zero, encontra-se a equação $X=0{,}64$. O que nos dá para o caminho de fibra 1 a seguinte solução:

$$\left|i0{,}4377sen\varphi e^{i\lambda}\alpha,\ i0{,}4377sen\varphi e^{i\lambda}\beta\right\rangle_2^1. \quad (2.23)$$

Pode ser visto na equação (2.23) que o segundo pulso a sair é o pulso correto. Com apenas operações passivas foi possível obter a informação correta com 19,16% da sua potência original, considerando um canal sem perdas. A energia total está distribuída entre os braços 1 e 2. Com $19{,}16\,sen^2\varphi$ % sai o pulso correto no braço 1 e com $19{,}16\cos^2\varphi$ % sai o pulso correto no braço 2.

No sistema da Figura 2.4, pode-se usar o primeiro pulso como habilitador para a detecção do segundo. Depois de detectado o segundo pulso, o sistema de detecção é desabilitado até que não haja mais luz dentro do anel. Depois deste período, o esquema de detecção passa a esperar um novo pulso de habilitação para uma nova detecção útil.

O modelo da Figura 2.4 embora corrija a variação aleatória da polarização, apresenta algumas dificuldades experimentais devido aos anéis ópticos na saída do esquema. Com o objetivo de obter um sistema mais prático, no sentido de que exija menos ou nenhum controle na detecção, propomos uma segunda configuração apresentada na Figura 2.5.

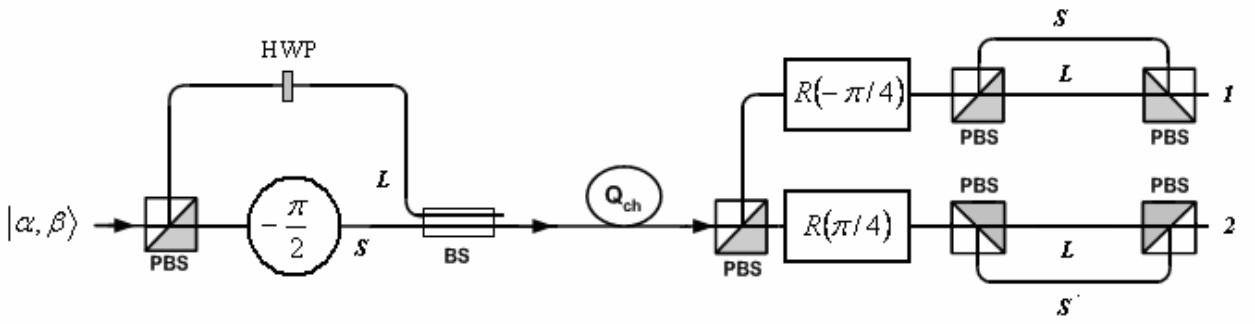

Figura 2.5 – Esquema II do sistema de correção de erro usando dispositivos ópticos passivos para comunicação quântica com estados coerentes.

Na Figura 2.5 BS é um divisor de feixe balanceado com transmitância $T = 1/\sqrt{2}$ e refletância $R = i/\sqrt{2}$. O esquema trabalha sobre um feixe polarizado representado pelo estado de entrada $|\alpha,\beta\rangle$ como se segue: As componentes do estado inicial são separadas pelo primeiro PBS. A componente horizontal percorre o caminho curto (S), recebendo a fase $-\pi/2$, enquanto a componente vertical percorre o caminho longo, passando através de um HWP (placa de meia onda), resultando em $|-i\alpha,0\rangle_S \otimes |\beta,0\rangle_L$. Após a passagem por um divisor de feixe balanceado, ambos os pulsos são lançados no canal quântico, separados pelo intervalo de tempo entre o pulso curto e o pulso longo. O estado de entrada no canal é $|\alpha/\sqrt{2},0\rangle_S \otimes |\beta/\sqrt{2},0\rangle_L$. Após a propagação desses pulsos no canal temos:

$$\left|\frac{\alpha}{\sqrt{2}}\cos(\varphi)e^{i\lambda},\frac{\alpha}{\sqrt{2}}\sin(\varphi)e^{i\xi}\right\rangle_S \otimes \left|\frac{\beta}{\sqrt{2}}\cos(\varphi)e^{i\lambda},\frac{\beta}{\sqrt{2}}\sin(\varphi)e^{i\xi}\right\rangle_L . \qquad (2.24)$$

Em que φ, λ e ξ são parâmetros de uma geral transformação unitária que atua sobre os dois pulsos. Sendo os sob escritos S e L indicativos dos pulsos recebidos no decodificador. Suas componentes são separadas pelo PBS, resultando no seguinte estado:

$$\left|\frac{\alpha}{\sqrt{2}}\cos(\varphi)e^{i\lambda},0\right\rangle_S^2 \otimes \left|0,\frac{\alpha}{\sqrt{2}}\sin(\varphi)e^{i\xi}\right\rangle_S^1 \otimes \left|\frac{\beta}{\sqrt{2}}\cos(\varphi)e^{i\lambda},0\right\rangle_L^2 \otimes \left|0,\frac{\beta}{\sqrt{2}}\sin(\varphi)e^{i\xi}\right\rangle_L^1. \quad (2.25)$$

Em que as componentes verticais viajam pelo caminho 1 e as componentes horizontais viajam pelo caminho 2. Olhando apenas para o caminho 1, há um rotacionador de polarização de com ângulo $-\pi/4$, $R(-\pi/4)$, resultando em:

$$\left|\frac{\alpha}{2}\sin(\varphi)e^{i\xi},\frac{\alpha}{2}\sin(\varphi)e^{i\xi}\right\rangle_S^1 \otimes \left|\frac{\beta}{2}\sin(\varphi)e^{i\xi},\frac{\beta}{2}\sin(\varphi)e^{i\xi}\right\rangle_L^1. \quad (2.26)$$

No interferômetro após o rotacionador, as componentes são separadas pelo PBS. A componente vertical percorre o caminho curto S, enquanto a componente horizontal percorre o caminho longo L. Após o último PBS, o estado resultante na saída do percurso 1 é:

$$\left|0,\frac{\alpha}{2}\sin(\varphi)e^{i\xi}\right\rangle_{SS}^1 \otimes \left|\frac{\alpha}{2}\sin(\varphi)e^{i\xi},\frac{\beta}{2}\sin(\varphi)e^{i\xi}\right\rangle_{SL}^1 \otimes \left|\frac{\beta}{2}\sin(\varphi)e^{i\xi},0\right\rangle_{LL}^1. \quad (2.27)$$

Em uma análise similar, olhando para as componentes que viajam pelo caminho 2. Após a passagem pelo rotacionador de ângulo de $\pi/4$ e um interferômetro idêntico ao existente no caminho 1, o estado de saída no caminho 2 é:

$$\left|0,\frac{\alpha}{2}\cos(\varphi)e^{i\lambda}\right\rangle_{SS}^2 \otimes \left|\frac{\alpha}{2}\cos(\varphi)e^{i\lambda},\frac{\beta}{2}\cos(\varphi)e^{i\lambda}\right\rangle_{SL}^2 \otimes \left|\frac{\beta}{2}\cos(\varphi)e^{i\lambda},0\right\rangle_{LL}^2. \quad (2.28)$$

Como pode ser observado em (2.27) e (2.28), em cada saída haverá três pulsos, sendo que o pulso no tempo central, *LS*, possui a mesma polarização do pulso enviado no transmissor. Percebemos que 1/4 da energia do pulso de entrada corresponde a energia do pulso corrigido na saída para o caso de uma fibra sem perdas.

CAPÍTULO 3

Análise de segurança de um sistema de distribuição quântica de chaves empregando correção de erro quântico

3.1 Introdução

Nos protocolos de distribuição quântica de chaves (DQC) em canais ruidosos, a taxa de erro de canal, que é uma componente da taxa de erro do sistema, é uma informação essencial para a garantia de segurança da comunicação. Quando uma espionagem é realizada a taxa de erro na comunicação aumenta. Entretanto, o erro causado por um espião é indistinguível do erro causado por componentes não ideais. Isto obriga a existência de uma margem de tolerância ao erro nos protocolos de DQC para tomar a decisão de realizar ou não a troca de chaves [47]. Portanto, é importante analisar o impacto da introdução do sistema de correção de erros na segurança do sistema de DQC. Nesta direção, este capítulo considera a análise de segurança de um sistema de DQC, executando o protocolo BB84 e utilizando a polarização de fótons isolados, quando do uso de um sistema de correção quântica de erros, como apresentado no Capítulo 2.

3.2 Sistema de correção de erro

O sistema de correção de erro considerado é uma versão simplificada das configurações mostradas no Capítulo 2. A arquitetura deste sistema, proposta em [42], é mostrada na Figura 3.1.

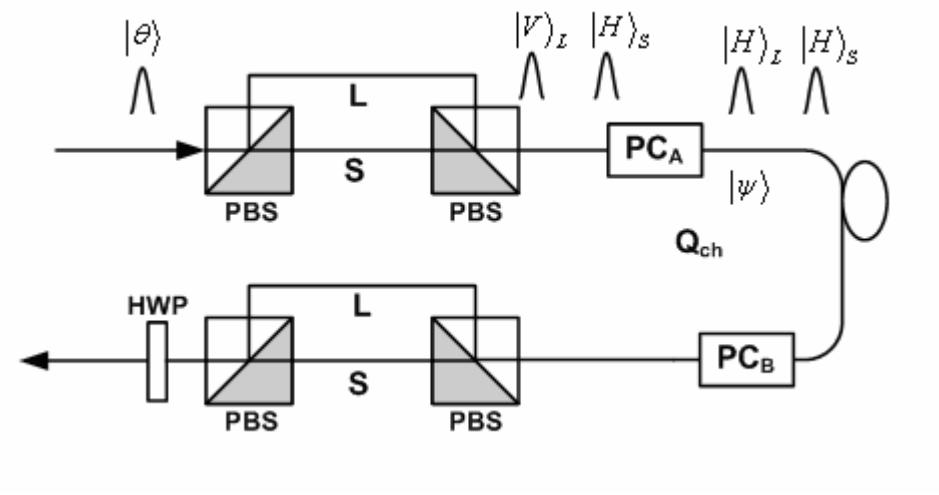

Figura 3.1 – Esquema óptico utilizado para realizar a correção de erro quântico.

O estado quântico na entrada do esquema mostrado na Figura 3.1 é $|\theta\rangle=a|H\rangle+b|V\rangle$. Após passar pelo IP no transmissor, $|\theta\rangle$ é transformado em:

$$\left|\theta'\right\rangle = a\left|H\right\rangle_S + b\left|V\right\rangle_L . \tag{3.1}$$

A célula de Pockels PC_A atua rotacionando de $\pi/2$ somente o pulso que percorre o caminho longo. Portanto, o pulso na entrada do canal óptico é:

$$\left|\psi\right\rangle = a\left|H\right\rangle_S + b\left|H\right\rangle_L . \tag{3.2}$$

Sendo o canal óptico variante no tempo mais uma vez modelado pela operação unitária (2.4), o estado quântico na saída da fibra óptica é:

$$|\psi'\rangle = a\left[\cos(\varphi)|H\rangle_S + sen(\varphi)e^{i\lambda}|V\rangle_S\right] + b\left[\cos(\varphi)|H\rangle_L + sen(\varphi)e^{i\lambda}|V\rangle_L\right]. \quad (3.3)$$

Chegando no receptor, a ação da célula de Pockels PC_B é rotacionar de $\pi/2$ somente a componente do estado que chega primeiro (a que passou pelo caminho curto no transmissor). Assim, o estado quântico imediatamente antes do IP no receptor é

$$|\psi''\rangle = a\left[\cos(\varphi)|V\rangle_S + sen(\varphi)e^{i\lambda}|H\rangle_S\right] + b\left[\cos(\varphi)|H\rangle_L + sen(\varphi)e^{i\lambda}|V\rangle_L\right]. \quad (3.4)$$

Após a passagem pelo IP do receptor, o estado resultante é:

$$|\psi'''\rangle = \cos(\varphi)\left[a|V\rangle_{SL} + b|H\rangle_{LS}\right] + sen(\varphi)e^{i\lambda}\left[a|H\rangle_{SS} + b|V\rangle_{LL}\right]. \quad (3.5)$$

Por fim, após a placa de meia onda, o estado quântico na saída é:

$$|\Phi\rangle = \cos(\varphi)\left[a|H\rangle_{Sl} + b|V\rangle_{LS}\right] + sen(\varphi)e^{i\lambda}\left[a|V\rangle_{SS} + b|H\rangle_{LL}\right]. \quad (3.6)$$

Da equação (3.6) observa-se que, com probabilidade $\cos^2(\varphi)$ o estado correto de polarização aparece no instante de tempo central *LS*. Por outro lado, com probabilidade $\text{sen}^2(\varphi)$ o estado de polarização aparece no instante de tempo *LL* (horizontal) ou no instante de tempo *SS* (vertical), indicando que houve um erro. Como φ é um parâmetro do canal, seu valor é totalmente estatístico por conta da variação aleatória da birrefringência do canal. Então podemos calcular

uma média para uma distribuição normal de φ no intervalo (0,2π), temos $\langle\cos^2(\varphi)\rangle = \langle\text{sen}^2(\varphi)\rangle = 1/2$. O que nos diz que para uma quantidade suficientemente grande de qubits enviados, metade deles serão medidos no instante *SL*.

3.3. Protocolo BB84 com sistema de correção de erro quântico

O protocolo BB84 executado em uma rede óptica contendo o sistema de correção de erros quântico da Figura 3.1 deve funcionar da seguinte maneira:

1. Alice escolhe aleatoriamente 4*n* bits de dados gerando a seqüência $a = \{a_1, a_2, \cdots, a_{4n}\}$.
2. Alice escolhe aleatoriamente uma seqüência $b = \{b_1, b_2, \cdots, b_{4n}\}$ de 4*n* bits. Cada bit b_k codifica um bit de dado a_k em umas das bases $B_0 \{|H\rangle, |V\rangle\}$ ou $B_1 \{|\pi/4\rangle, |3\pi/4\rangle\}$.
3. Alice envia para Bob uma seqüência de qubits codificados na polarização de fótons isolados. O conjunto inteiro é representado pelo estado $|\theta_T\rangle = \bigotimes_{k=1}^{4n} |\theta_{a_k,b_k}\rangle$ sendo $|\theta_{00}\rangle=|H\rangle$, $|\theta_{01}\rangle=|V\rangle$, $|\theta_{10}\rangle=|\pi/4\rangle$ e $|\theta_{11}\rangle=|3\pi/4\rangle$. Os estados são enviados um de cada vez.
4. Cada fóton recebido por Bob é medido em uma base (B_0 ou B_1) escolhida aleatoriamente.
5. Bob revela publicamente quais bits ele detectou na janela de tempo central *LS*. Os não recebidos nesta janela de tempo são descartados. Em média restarão $4n\langle\cos^2(\varphi)\rangle$ bits.
6. Alice e Bob revelam publicamente as seqüências de bases que utilizaram para os bits que restaram.
7. Alice e Bob descartam todos os bits para os quais escolheram bases diferentes. Em média restarão $2n\langle\cos^2(\varphi)\rangle$ bits.
8. Alice escolhe um subconjunto de, por exemplo, metade dos bits restantes, e diz para Bob quais bits selecionou. Alice e Bob comparam as seqüências de bits verificadores, em

média $n\langle\cos^2(\varphi)\rangle$ bits, e se houver discordância acima do limite aceitável o protocolo é abortado, pois fica caracterizada a presença de um espião.

9. Se a taxa de erro dos bits comparados for menor que o limite de segurança estabelecido, restaram, em média $n\langle\cos^2(\varphi)\rangle$ bits. Então Alice e Bob executam os protocolos clássicos de correção de erro e amplificação de privacidade.

3.4. O ataque da espiã Eva

Eva é a espiã que realiza a interceptação, na entrada do canal óptico, dos estados quânticos enviados por Alice. O objetivo de Eva é obter o máximo de informação que comporá a chave criptográfica a ser distribuída. Para isso, Eva tem que escolher o tipo de ataque que realizará no sistema óptico por onde trafegam os dados de Alice e Bob. O ataque mais geral que Eva pode realizar consiste em entrelaçar o fóton enviado por Alice com um outro fóton, providenciado por Eva, através de uma operação unitária. Eva envia um dos fótons a Bob e faz uma medição no outro. As quantidades de informação que Eva ganha e de distúrbio que Eva causa dependem do estado inicial do fóton de Eva, da operação unitária e da medição que Eva escolhe. O ataque ótimo, ou seja, com os parâmetros que maximizam a informação ganha e minimizam os distúrbios causados por Eva está mostrado na Figura 3.2 [48,49].

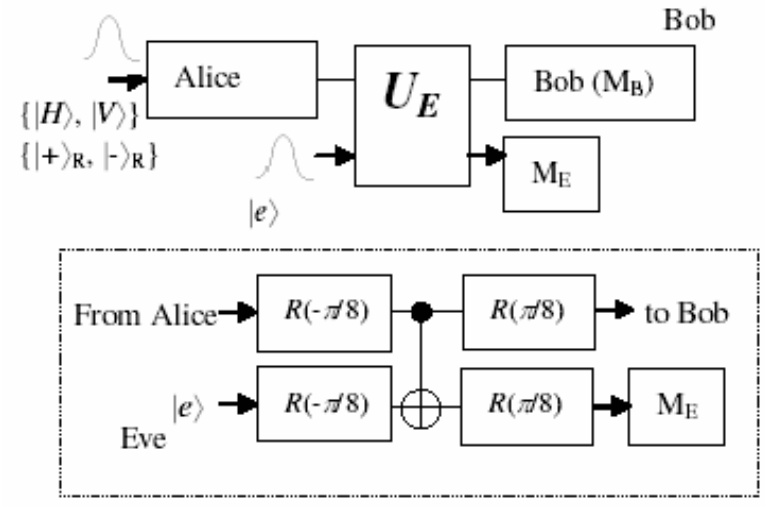

Figura 3.2 – Estratégia de espionagem Fuchs-Peres-Brandt.

Na Figura 3.2, Alice e Bob executam o protocolo BB84 com estados de polarização na base retangular ($|H\rangle$,$|V\rangle$) e diagonal ($|+\rangle_R=(|H\rangle+|V\rangle)/2^{1/2}=|\pi/4\rangle$, $|-\rangle_R=(|H\rangle-|V\rangle)/2^{1/2}=|3\pi/4\rangle$), R é um rotacionador de polarização, a operação unitária U_E é composta por quatro rotacionadores R e uma CNOT, M_E é o medidor de Eva e $|e\rangle$ é o estado quântico do fóton de Eva, dado por;

$$|e\rangle = C|+\rangle + S|-\rangle\,, \tag{3.7}$$

$$C = \sqrt{1-2P_E}\ ,\ S = \sqrt{2P_E}\ , \tag{3.8}$$

$$|\pm\rangle = \left(|0\rangle \pm |1\rangle\right)/\sqrt{2}\,, \tag{3.9}$$

$$|0\rangle = \cos(\pi/8)|H\rangle + \sin(\pi/8)|V\rangle, \tag{3.10}$$

$$|1\rangle = -\sin(\pi/8)|H\rangle + \cos(\pi/8)|V\rangle\,. \tag{3.11}$$

Observando (3.7) e (3.8), pode-se notar que o estado inicial do fóton de Eva é parametrizado pela probabilidade P_E de Eva causar um erro em Bob. A base $\{|0\rangle,|1\rangle\}$ em (3.10) e (3.11) é a base de medição usada por Eva. Para cada possível escolha de Alice, o estado conjunto de Alice-Eva é;

$$U_E|H\rangle|e\rangle = |H\rangle|T_-\rangle + |V\rangle|T_E\rangle, \tag{3.12}$$
$$U_E|H\rangle|e\rangle = |V\rangle|T_+\rangle + |H\rangle|T_E\rangle, \tag{3.13}$$
$$U_E|+\rangle_R|e\rangle = |+\rangle_R|T_+\rangle + |-\rangle_R|T_E\rangle, \tag{3.14}$$
$$U_E|-\rangle_R|e\rangle = |-\rangle_R|T_-\rangle + |+\rangle_R|T_E\rangle. \tag{3.15}$$

Em (3.12)-(3.15) $|T_\pm\rangle$ e $|T_E\rangle$ são os estados não normalizados;

$$|T_\pm\rangle = C|+\rangle \pm \left(S/\sqrt{2}\right)|-\rangle, \tag{3.16}$$
$$|T_E\rangle = \left(S/\sqrt{2}\right)|-\rangle. \tag{3.17}$$

Como pode ser visto nas equações (3.12) a (3.15), a probabilidade de ocorrer um erro, para $X \in \{H,V,+_R,-_R\}$ é igual a $\langle X^\perp,T_E|U_E|X,e\rangle = \langle X^\perp,T_E|X,T_\pm\rangle + \langle X^\perp,T_E|X^\perp,T_E\rangle = \langle T_E|T_E\rangle = S^2/2 = P_E$. É fácil de verificar que a probabilidade de Eva capturar um resultado correto em sua medição, para cada fóton enviado por Alice, é $0{,}5(1+2^{1/2}CS)$. Se Eva escolhe $P_E = 0$ or 0,5, então a probabilidade de Eva capturar o valor correto é de 0,5. Para $P_E = 0{,}25$, temos a máxima probabilidade de sucesso que é 0,8535.

Quando a rede óptica a ser atacada por Eva possui o sistema de correção de erros mostrado na Figura 3.1, Eva deve, inicialmente, possuir o mesmo codificador e decodificador usado por Alice e Bob, respectivamente. Eva decodifica o estado quântico codificado por Alice recuperando com alta probabilidade (dado que Eva está bem na entrada do canal) o estado de polarização correto. Então, ela realiza o ataque Fuchs-Peres-Brandt, codifica o fóton e o envia para Bob. Se o estado enviado por Alice foi, sem perda de generalidade, $|+\rangle_R$, então o estado após a atuação de ataque de Eva, propagação no canal ruidoso e decodificação de Bob é:

$$|\Phi\rangle = \cos(\varphi)\left[|+\rangle_{RLS}|T_\pm\rangle - |-\rangle_{RLS}|T_E\rangle\right] + \sin(\varphi)e^{i\lambda}\left[\left(\frac{|H\rangle_{SS}+|V\rangle_{LL}}{\sqrt{2}}\right)|T_\pm\rangle + \left(\frac{|H\rangle_{SS}-|V\rangle_{LL}}{\sqrt{2}}\right)|T_E\rangle\right]. \tag{3.18}$$

Observando a equação (3.18) podemos concluir que, nos casos em que não há erro na comunicação (detecção no tempo *SL*) haverá uma probabilidade de erro igual a P_E que representa exclusivamente a ação de Eva. Com esta composição, pode-se notar que a distribuição quântica de chaves em um canal ruidoso ocorrerá como se o canal fosse ideal, dando às partes legítimas da comunicação uma maior segurança quanto à presença de Eva. Assim, o ato de espionagem, é o único agente redutor de informação mútua na distribuição quântica de chaves entre Alice e Bob. Toda a análise feita neste capítulo considera que a única fonte de ruído é o canal. Entretanto, em sistemas reais, fontes de ruídos estão presentes em todas as partes, transmissor, canal e receptor.

Uma outra opção é usando o sistema de correção de erro mostrado na Figura 2.3. Como vantagem é que esse sistema de correção pode ser aplicado no protocolo BB84 sem necessidades de alterações no protocolo. O ataque de Eva é analisado como segue: Suponha-se, sem perda de generalidade, que Alice enviou o estado quântico $|+\rangle_R$, então a evolução do estado quântico da saída de Eva até a saída de Bob é como segue:

1. Estado na saída de Eva (ou na entrada do canal óptico)

$$\frac{\left(|H\rangle_S + |H\rangle_L\right)}{\sqrt{2}}|T_+\rangle + \frac{\left(|H\rangle_S - |H\rangle_L\right)}{\sqrt{2}}|T_E\rangle \tag{3.19}$$

2. Estado após a propagação na fibra óptica (ou na entrada de Bob)

$$\left\{\frac{\left[\cos(\varphi)e^{i\lambda}|H\rangle_S + \sin(\varphi)e^{i\xi}|V\rangle_S\right]}{\sqrt{2}} + \frac{\left[\cos(\varphi)e^{i\lambda}|H\rangle_L + \sin(\varphi)e^{i\xi}|V\rangle_L\right]}{\sqrt{2}}\right\}|T_+\rangle +$$
$$\left\{\frac{\left[\cos(\varphi)e^{i\lambda}|H\rangle_S + \sin(\varphi)e^{i\xi}|V\rangle_S\right]}{\sqrt{2}} - \frac{\left[\cos(\varphi)e^{i\lambda}|H\rangle_L + \sin(\varphi)e^{i\xi}|V\rangle_L\right]}{\sqrt{2}}\right\}|T_E\rangle \tag{3.20}$$

3. Estado após o primeiro PBS em Bob

$$\frac{\left[\cos(\varphi)e^{i\lambda}|H\rangle_S^2 + \cos(\varphi)e^{i\lambda}|H\rangle_L^2\right]}{\sqrt{2}}|T_+\rangle + \frac{\left[\cos(\varphi)e^{i\lambda}|H\rangle_S^2 - \cos(\varphi)e^{i\lambda}|H\rangle_L^2\right]}{\sqrt{2}}|T_E\rangle +$$
$$\frac{\left[\sin(\varphi)e^{i\xi}|V\rangle_S^1 + \sin(\varphi)e^{i\xi}|V\rangle_L^1\right]}{\sqrt{2}}|T_+\rangle + \frac{\left[\sin(\varphi)e^{i\xi}|V\rangle_S^1 - \sin(\varphi)e^{i\xi}|V\rangle_L^1\right]}{\sqrt{2}}|T_E\rangle \tag{3.21}$$

4. Estado após as células de Pockels PC_{B1} e PC_{B2}

$$\frac{\left[\cos(\varphi)e^{i\lambda}\left|H\right\rangle_S^2+\cos(\varphi)e^{i\lambda}\left|V\right\rangle_L^2\right]}{\sqrt{2}}\left|T_+\right\rangle+\frac{\left[\cos(\varphi)e^{i\lambda}\left|H\right\rangle_S^2-\cos(\varphi)e^{i\lambda}\left|V\right\rangle_L^2\right]}{\sqrt{2}}\left|T_E\right\rangle+$$
$$\frac{\left[\sin(\varphi)e^{i\xi}\left|H\right\rangle_S^1+\sin(\varphi)e^{i\xi}\left|V\right\rangle_L^1\right]}{\sqrt{2}}\left|T_+\right\rangle+\frac{\left[\sin(\varphi)e^{i\xi}\left|H\right\rangle_S^1-\sin(\varphi)e^{i\xi}\left|V\right\rangle_L^1\right]}{\sqrt{2}}\left|T_E\right\rangle \quad (3.22)$$

5. Estado após os interferômetros de polarização (ou antes do medidor de Bob)

$$\left|\Psi\right\rangle=e^{i\lambda}\cos(\varphi)\left\{\frac{\left[\left|H\right\rangle_{SL}^2+\left|V\right\rangle_{LS}^2\right]}{\sqrt{2}}\left|T_+\right\rangle+\frac{\left[\left|H\right\rangle_{SL}^2-\left|V\right\rangle_{LS}^2\right]}{\sqrt{2}}\left|T_E\right\rangle\right\}+$$
$$e^{i\xi}\sin(\varphi)\frac{\left[\left|H\right\rangle_{SL}^1+\left|V\right\rangle_{LS}^1\right]}{\sqrt{2}}\left|T_+\right\rangle+\frac{\left[\left|H\right\rangle_{SL}^1-\left|V\right\rangle_{LS}^1\right]}{\sqrt{2}}\left|T_E\right\rangle \quad (3.23)$$
$$\left|\Psi\right\rangle=e^{i\lambda}\cos(\varphi)\left[\left|+\right\rangle_R^2\left|T_+\right\rangle+\left|-\right\rangle_R^2\left|T_E\right\rangle\right]+e^{i\xi}\sin(\varphi)\left[\left|+\right\rangle_R^1\left|T_+\right\rangle+\left|-\right\rangle_R^1\left|T_E\right\rangle\right] \quad (3.24)$$

Observando (3.24) pode-se concluir que mais uma vez que, mesmo quando não deveriam ocorrer erros, existirá uma probabilidade de erro igual a P_E (equação (3.8)) exclusivamente devida à ação de Eva. O mesmo ocorrerá para todas as demais possíveis escolhas de Alice. Assim, o esquema de correção de erro não tem qualquer influência no erro causado por Eva e, portanto, a ação de Eva fica mais visível.

Conclusões e Perspectivas

O Capítulo 1 pode ser dividido em duas partes, uma teórica e a outra experimental. Na primeira, uma revisão dos conceitos de polarização foi realizada, dando ênfase à despolarização. Uma simulação foi realizada mostrando a queda do grau de polarização durante a propagação da luz em um canal despolarizador. Na segunda parte, foi realizado um experimento para medir o grau de polarização de um estado coerente após propagação em um trecho de 200 m de fibra óptica bobinada. Os resultados experimentais obtidos mostram claramente a deterioração do poder de determinação da polarização provocado pela despolarização. Além disso, o valor do grau de polarização medido pode ser usado como parâmetro do canal despolarizador de qubits.

No Capítulo 2, foi analisado o sistema de correção de erro quântico apresentado na referência [42]. Baseado nele, dois outros sistemas foram proposto, sendo um passivo para sistemas de comunicação quântica que usam estados coerentes, e o outro ativo para sistemas de comunicação quântica que usam fótons isolados. Comparando este último com o da referência [42] pode-se verificar que, além de apresentar o mesmo desempenho, o esquema óptico de correção de erros quânticos proposto neste trabalho é mais simples de construir e de operar, pois tem menos componentes passivos e ativos (células de Pockels).

No Capítulo 3 foi analisada a segurança de um sistema de distribuição quântica de chaves polarimétrico, usando fótons isolados, quando o mesmo utiliza sistemas de correção de erro. O ataque escolhido para a análise foi o conhecido ataque de Fuchs-Peres-Brandt. Os resultados obtidos mostram que o sistema de correção de erros facilita a descoberta da presença de uma espiã, uma vez que o mesmo corrige os erros do canal mas não corrige os erros causados pela espiã.

Como trabalhos futuros, podem ser citados: 1) A inclusão da análise da dispersão de modos de polarização (PMD), com a modificação dos esquemas ópticos de correção propostos para também realizar a compensação da PMD permitindo, assim, melhorar a taxa de transmissão de bits úteis e a distância entre transmissor e receptor. 2) A utilização do esquema de correção de erro em sistemas de distribuição de fótons entrelaçados.

APÊNDICE A

Dispersão dos modos de polarização

Em uma fibra monomodo, uma luz com qualquer estado de polarização pode ser representada como uma combinação linear dos dois modos ortogonais HE_{11} linearmente polarizados. Em uma fibra óptica perfeita (isotrópica e com simetria cilíndrica), estes modos são degenerados, isto é, possuem a mesma constante de propagação. Em fibras reais, defeitos causados durante o processo de fabricação da fibra como a não perfeita circularidade do núcleo e/ou da casca causa o aparecimento de eixos principais, nos quais a luz se decompõe, e que possuem diferentes índices de refração, isto é, a fibra se torna birrefringente. Neste caso os modos acima citados não são mais degenerados e a fibra se torna bimodal.

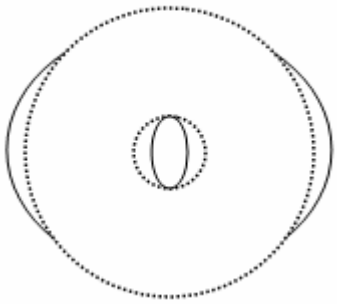

Figura A.1 – Fibra óptica não ideal com núcleo e casca de formato oval.

A birrefringência pode também ser induzida por estresse mecânico externo (por exemplo, pressão na fibra exercida por pesos) e interno (por exemplo, causado pela diferença do coeficiente de expansão térmico dos materiais constituintes do núcleo e da casca), encurvamento e torção na fibra. Em fibras ópticas instaladas estes efeitos ocorrem aleatoriamente em relação ao tempo e ao

longo da fibra. A diferença no índice de refração causada pela birrefringência é da ordem de 10^{-5}-10^{-7}, enquanto que a diferença dos índices de refração do núcleo e da casca da fibra é da ordem de 10^{-3}. Mesmo pequena, a diferença dos índices de refração é suficiente para deteriorar o desempenho dos sistemas modernos de comunicações ópticas.

A modelagem de um longo comprimento de fibra é realizado considerando a concatenação de pequenos trechos de fibra nos quais, por um determinado intervalo de tempo, a birrefringência é considerada constante. Em um destes trechos a fibra possui dois eixos de propagação e cada eixo possui seu próprio índice de refração, digamos n_r (índice rápido) e n_l (índice lento), $n_l > n_r$. Assim, a diferença na constante de propagação dos dois modos é:

$$\beta_l - \beta_r = \frac{\omega(n_l - n_r)}{C} = \frac{\omega \Delta n}{C}. \tag{A.1}$$

onde ω é a freqüência angular da luz e C é a velocidade da luz no vácuo. Quando ambos os modos são excitados na entrada da fibra óptica a polarização da luz varia ao longo do comprimento da fibra e, após um comprimento chamado *comprimento de batimento* (beat length) a polarização inicial é recuperada. O comprimento de batimento é determinado pela condição:

$$\phi_x = \phi_{x0} + \beta_l L \tag{A.2}$$
$$\phi_y = \phi_{y0} + \beta_r L \tag{A.3}$$
$$\phi_x - \phi_y = \phi_{x0} - \phi_{y0} + (\beta_l - \beta_r)L = \phi_{x0} - \phi_{y0} + 2\pi \tag{A.4}$$

onde ϕ_x é a fase do modo lento composta pela fase inicial ϕ_{x0} somada à fase adquirida durante a propagação $\beta_l L$, enquanto que ϕ_y é a fase do modo rápido composta pela fase inicial ϕ_{y0} somada à fase adquirida durante a propagação $\beta_r L$. Da equação (A.4) vemos que o comprimento de batimento é dado por:

$$L_B = \frac{2\pi}{(\beta_l - \beta_r)} = \frac{2\pi C}{\omega \Delta n} = \frac{\lambda}{\Delta n}. \tag{A.5}$$

A diferença na velocidade fase provoca uma diferença na velocidade de grupo dos modos o que, por sua vez, causa um atraso relativo na chegada dos modos ao fim da fibra chamado atraso diferencial de grupo, DGD (differential group delay). Um modo com constante de propagação β leva um tempo $(d\beta/d\omega)L$ para percorrer um comprimento L de fibra. No trecho de fibra birrefringente teremos então o atraso diferencial, por unidade de comprimento, dado por:

$$DGD = \frac{\Delta\tau}{L} = \frac{(\tau_l - \tau_r)}{L} = \frac{d(\beta_l - \beta_r)}{d\omega} = \frac{\Delta n}{C} - \frac{\omega}{C}\frac{d\Delta n}{d\omega} \tag{A.6}$$

A equação acima dá a dispersão de modo de polarização intrínseca de um trecho de fibra com birrefringência uniforme. O atraso varia linearmente com o comprimento de fibra apenas por que não há acoplamento entre os dois modos. A equação acima mostra-nos ainda que há uma dependência do estado de polarização na saída do trecho de fibra com a freqüência da onda óptica incidente. Para a mesma polarização na entrada da fibra, se a freqüência for variada, o vetor de Stokes se moverá sobre o perímetro de um círculo na superfície da esfera. Após uma determinada variação de freqüência $\Delta\omega$ a polarização inicial é recuperada. A relação entre $\Delta\tau$ e $\Delta\omega$ é:

$$\Delta\omega = \frac{2\pi}{\Delta\tau}. \tag{A.7}$$

Como afirmado anteriormente, a teoria acima é válida para trechos curtos de fibra. Entretanto, como podemos afirmar que um trecho é curto o suficiente para que a teoria seja aplicável? A resposta para esta pergunta é o comprimento de correlação L_c, que é o comprimento de fibra L_c tal que:

$$\frac{\langle P_i(L_c)\rangle - \langle P_o(L_c)\rangle}{P_i(0)} = \frac{1}{e^2}. \tag{A.8}$$

Na entrada na fibra a luz está toda polarizada na direção do eixo principal i com potência $P_i(0)$. Após a propagação em um comprimento L de fibra, mede-se a potência óptica da luz no eixo i, P_i, e a potência óptica da luz no eixo ortogonal o, P_o. Realizando várias vezes a medição

encontramos os valores onde médios $\langle P_i(L)\rangle$ e $\langle P_o(L)\rangle$. Quando $L=L_c$, (A.8) é satisfeita. A Fibra cujo comprimento é muito menor que L_c é considerada curta enquanto fibras com comprimento muito maior que L_c são consideradas longas, e a teoria do PMD intrínseco não é válida. Fibras enroladas em forma de bobina têm comprimento de correlação (~ 1m) muito menor que fibras esticadas (~ 1km).

A primeira tentativa de modelar PMD em fibras longas foi feita por Poole e Wagner [50], que desenvolveram a teoria dos estados principais de polarização (PSP). Este modelo pressupõe que o tempo de coerência da fonte luminosa é muito maior que os atrasos induzidos pelo PMD e que as perdas na fibra não são dependentes da polarização. A transmissão sobre uma fibra longa com birrefringência linear é representada pela matriz transferência;

$$U(\omega) = e^{\alpha(\omega)} \begin{bmatrix} u_1(\omega) & u_2(\omega) \\ -u_2^*(\omega) & u_1^*(\omega) \end{bmatrix}, \tag{A.9}$$

$$|u_1(\omega)|^2 + |u_2(\omega)|^2 = 1. \tag{A.10}$$

Em (A.9) $\alpha(\omega)$ representa a perda, igual para todos os estados de polarização. O estado de polarização na saída da fibra é dado por;

$$\begin{bmatrix} E_x^s \\ E_y^s \end{bmatrix} = U_f(\omega) \begin{bmatrix} E_x^e \\ E_y^e \end{bmatrix}, \tag{A.11}$$

$$|\psi_s(\omega)\rangle = U_f(\omega)|\psi_e\rangle. \tag{A.12}$$

Em (A.11), por exemplo, E_x^e é o campo elétrico na direção x na entrada da fibra. O estado de polarização na saída da fibra óptica, $|\psi_s(\omega)\rangle$, depende da freqüência óptica ω mesmo quando a polarização da luz na entrada da fibra não depende. Isto ocorre por que o operador evolução $U_f(\omega)$ é dependente da freqüência. Por conseqüência, um pulso com espectro largo será fortemente despolarizado pela fibra, pois cada componente espectral evoluirá para um diferente estado de polarização. O grau de polarização da luz após a propagação depende das características da fibra, da largura espectral do pulso incidente e do estado de polarização da componente espectral central da saída $|\psi_s(\omega_0)\rangle$ e, portanto, depende do estado de polarização do

pulso na entrada, $|\psi_e\rangle = [U_f(\omega)]^{-1}|\psi_s(\omega_0)\rangle$. É fácil percebe que, se $|\psi_s(\omega)\rangle$ varia rapidamente quando ω varia ao redor de ω_0, então a despolarização é grande. Por outro lado, se $|\psi_s(\omega)\rangle \approx |\psi_s(\omega_0)\rangle$ para todo ω do espectro do pulso, então a despolarização é menor. De fato, a condição ótima, isto é, mínima despolarização, ocorre quando $|\psi_s(\omega)\rangle = e^{i\phi(\omega)}|\psi_s(\omega_0)\rangle$. A questão é, qual o estado $|\psi_e\rangle$, chamado de estado principal de polarização (PSP), tal que:

$$\left|\psi_s\left(\omega_0+\delta\omega\right)\right\rangle = e^{i\delta\omega\frac{\Delta\tau}{2}}\left|\psi_s\left(\omega_0\right)\right\rangle = e^{i\delta\omega\frac{\Delta\tau}{2}}U\left(\omega_0\right)^{-1}\left|\psi_e\right\rangle. \tag{A.13}$$

seja satisfeita? Para encontramos a solução partimos da derivada de (A.12):

$$\frac{d\left|\psi_s\left(\omega\right)\right\rangle}{d\omega} = \frac{dU_f\left(\omega\right)}{d\omega}\left|\psi_e\right\rangle = \frac{dU_f\left(\omega\right)}{d\omega}U_f\left(\omega\right)^{-1}\left|\psi_s\left(\omega\right)\right\rangle. \tag{A.14}$$

Na ausência de PDL, o operador evolução $U_f(\omega)$ é unitário e, portanto, $[U_f(\omega)]^{-1} = [U_f(\omega)]^{\dagger}$. Além disso, como $U_f(\omega)[U_f(\omega)]^{\dagger} = I$, temos que:

$$\frac{d\left[U_f\left(\omega\right)U_f\left(\omega\right)^{\dagger}\right]}{d\omega} = \frac{dU_f\left(\omega\right)}{d\omega}U_f\left(\omega\right)^{\dagger} + U_f\left(\omega\right)\frac{dU_f\left(\omega\right)^{\dagger}}{d\omega} = 0 \tag{A.15}$$

$$\frac{dU_f\left(\omega\right)}{d\omega}U_f\left(\omega\right)^{\dagger} = -U_f\left(\omega\right)\frac{dU_f\left(\omega\right)^{\dagger}}{d\omega} \tag{A.16}$$

A equação (A.16) mostra que o operador $i\frac{dU_f\left(\omega\right)}{d\omega}U_f\left(\omega\right)^{\dagger}$ é um operador auto-adjunto, isto é, ele tem autovalores reais e dois autovetores ortogonais entre si. Usando este fato em (A.14) temos que, se $|\psi_s(\omega)\rangle$ é autovetor de $\frac{dU\left(\omega\right)}{d\omega}U\left(\omega\right)^{\dagger}$ com autovalor $i\delta\tau/2$, então (A.14) fica da forma:

$$\frac{d\left|\psi_s\left(\omega\right)\right\rangle}{d\omega} = \frac{dU\left(\omega\right)}{d\omega}U\left(\omega\right)^{\dagger}\left|\psi_s\left(\omega\right)\right\rangle = -i\frac{\delta\tau}{2}\left|\psi_s\left(\omega\right)\right\rangle. \tag{A.17}$$

Cuja solução é facilmente encontrada como sendo:

$$\left|\psi_s\left(\omega\right)\right\rangle = e^{-i\frac{\Delta\tau}{2}\left(\omega-\omega_0\right)}\left|\psi_s\left(\omega=\omega_0\right)\right\rangle = e^{-i\frac{\Delta\tau}{2}\delta\omega}\left|\psi_s\left(\omega_0\right)\right\rangle. \tag{A.18}$$

O valor $\Delta\tau$ é real e representa o atraso diferencial de grupo (DGD). Portanto, os dois autovetores do operador $\frac{dU\left(\omega\right)}{d\omega}U\left(\omega\right)^{\dagger}$ são os estados principais de polarização. Se a luz que entra na fibra tem estado de polarização coincidente com um dos estados principais, a luz na saída fibra óptica terá polarização independente, em primeira ordem, da freqüência.

APÊNDICE B

Operador quântico de rotação para o estado coerente bimodal

O operador quântico de rotação para o estado coerente bimodal é $e^{i\theta\hat{S}_3}$, sendo $\hat{S}_3 = a^\dagger b - ab^\dagger$ um operador quântico de Stokes e, a e b, os operadores aniquilação dos modos. O cálculo do estado coerente bimodal na saída para o estado $|\alpha\rangle|\beta\rangle$ na entrada, para uma rotação de um ângulo θ é como se segue:

$$\begin{aligned} e^{i\theta\hat{S}_3}|\alpha\rangle|\beta\rangle &= e^{i\theta\hat{S}_3}\left(e^{-\frac{|\alpha|^2}{2}}\sum_{n=0}^{\infty}\frac{\alpha^n}{\sqrt{n!}}|n\rangle\right)\left(e^{-\frac{|\beta|^2}{2}}\sum_{m=0}^{\infty}\frac{\beta^m}{\sqrt{m!}}|m\rangle\right) \\ &= e^{i\theta\hat{S}_3}\left(e^{-\frac{|\alpha|^2}{2}}\sum_{n=0}^{\infty}\frac{\alpha^n}{\sqrt{n!}}\frac{\left(a^\dagger\right)^n}{\sqrt{n!}}|0\rangle\right)\left(e^{-\frac{|\beta|^2}{2}}\sum_{m=0}^{\infty}\frac{\beta^m}{\sqrt{m!}}\frac{\left(b^\dagger\right)^m}{\sqrt{m!}}|0\rangle\right) \\ &= e^{-\frac{|\alpha|^2+|\beta|^2}{2}}\sum_{n=0}^{\infty}\sum_{m=0}^{\infty}\frac{\alpha^n}{\sqrt{n!}}\frac{\beta^m}{\sqrt{m!}}e^{i\theta\hat{S}_3}\frac{\left(a^+\right)^n}{\sqrt{n!}}\frac{\left(b^+\right)^m}{\sqrt{m!}}|0\rangle|0\rangle\,, \end{aligned} \tag{B.1}$$

sendo

$$e^{i\theta\hat{S}_3}\frac{\left(a^\dagger\right)^n}{\sqrt{n!}}\frac{\left(b^\dagger\right)^m}{\sqrt{m!}} = \frac{\left(e^{i\theta\hat{S}_3}a^\dagger e^{-i\theta\hat{S}_3}\right)^n}{\sqrt{n!}}\frac{\left(e^{i\theta\hat{S}_3}b^\dagger e^{-i\theta\hat{S}_3}\right)^m}{\sqrt{m!}}\,. \tag{B.2}$$

Usando a fórmula de Baker-Campbell-Hausdorf pode-se desenvolver a relação B.2 da seguinte forma [51]:

$$e^{i\theta\hat{S}_3}a^\dagger e^{-i\theta\hat{S}_3} = \sum_{p=0}^{\infty}\frac{\theta^p}{p!}C_p \ . \tag{B.3}$$

Em (B.3) $C_p = \left[i\theta\hat{S}_3, C_{p-1}\right]$, sendo $C_0 = a^\dagger$. Sabendo que $-b^\dagger = \left[a^\dagger b - ab^\dagger, a^\dagger\right]$ e $a^\dagger = \left[a^\dagger b - ab^\dagger, b^\dagger\right]$, a operação de comutação se torna cíclica para C_p, de forma que $C_{par} = i^p a^\dagger$ e $C_{impar} = i^{p+1}b^\dagger$. Pode-se então desenvolver a seguinte série:

$$\sum_{p=0}^{\infty}\frac{\theta^p}{p!}C_p = \sum_{p=par}^{\infty}\frac{\theta^p}{p!}i^p a^\dagger + \sum_{p=ímpar}^{\infty}\frac{\theta^p}{p!}i^{p+1}b^\dagger \ . \tag{B.4}$$

Fazendo a abreviação $p(t) = \begin{cases} 2t & par \\ 2t+1 & ímpar \end{cases}$, tem-se que:

$$\begin{aligned} &\sum_{t=0}^{\infty}\frac{\theta^{2t}}{(2t)!}i^{2t}a^\dagger + \sum_{t=0}^{\infty}\frac{\theta^{2t+1}}{(2t+1)!}i^{2t+1+1}b^\dagger \\ &= \sum_{t=0}^{\infty}\frac{(-1)^t\theta^{2t}}{(2t)!}a^\dagger + \sum_{t=0}^{\infty}\frac{(-1)^{t+1}\theta^{2t+1}}{(2t+1)!}b^\dagger \\ &= \cos(\theta)a^\dagger + \sin(\theta)b^\dagger . \end{aligned} \tag{B.5}$$

Resolvendo, agora, para $\left(e^{i\theta\hat{S}_3}b^\dagger e^{-i\theta\hat{S}_3}\right)^n$, tem-se $C_{par} = i^p b^\dagger$ e $C_{impar} = -(i)^{p+1}a^\dagger$, o que leva à seguinte série:

$$\sum_{p=0}^{\infty}\frac{\theta^p}{p!}C_p = \sum_{p=par}^{\infty}\frac{\theta^p}{p!}i^p b^\dagger - \sum_{p=ímpar}^{\infty}\frac{\theta^p}{p!}i^{p+1}a^\dagger \ . \tag{B.6}$$

A parametrização de funções pares e ímpares na reta é *par* = 2*t* e *ímpar* = 2*t*+1, obtém-se o seguinte desenvolvimento:

$$\begin{aligned}&\sum_{t=0}^{\infty}\frac{\theta^{2t}}{(2t)!}i^{2t}a^{\dagger}-\sum_{t=0}^{\infty}\frac{\theta^{2t+1}}{(2t+1)!}i^{2t+1+1}b^{\dagger}\\&=\sum_{t=0}^{\infty}\frac{(-1)^{t}\theta^{2t}}{(2t)!}b^{\dagger}-\sum_{t=0}^{\infty}\frac{(-1)^{t+1}\theta^{2t+1}}{(2t+1)!}a^{\dagger}\\&=\cos(\theta)b^{\dagger}-\sin(\theta)a^{\dagger}.\end{aligned}\tag{B.7}$$

Como $e^{i\theta\hat{S}_3}a^{\dagger}e^{-i\theta\hat{S}_3}=a^{\dagger}\cos(\theta)+b^{\dagger}\sin(\theta)$ e $e^{i\theta\hat{S}_3}b^{\dagger}e^{-i\theta\hat{S}_3}=b^{\dagger}\cos(\theta)-a^{\dagger}\sin(\theta)$, tem-se que:

$$e^{-\frac{|\alpha|^2+|\beta|^2}{2}}\sum_{n=0}^{\infty}\sum_{m=0}^{\infty}\frac{\alpha^n}{\sqrt{n!}}\frac{\beta^m}{\sqrt{m!}}\frac{\left(a^{\dagger}\cos(\theta)+b^{\dagger}\sin(\theta)\right)^n}{\sqrt{n!}}\frac{\left(b^{\dagger}\cos(\theta)-a^{\dagger}\sin(\theta)\right)^m}{\sqrt{m!}}|0\rangle|0\rangle.\tag{B.8}$$

Sabemos da seguinte relação binomial;

$$\left(a^{\dagger}\cos(\theta)+b^{\dagger}\sin(\theta)\right)^n=\sum_{i=0}^{n}\binom{n}{i}\left(a^{\dagger}\cos(\theta)\right)^{n-i}\left(b^{\dagger}\sin(\theta)\right)^i,\tag{B.9}$$

$$\left(b^{\dagger}\cos(\theta)-a^{\dagger}\sin(\theta)\right)^m=\sum_{j=0}^{m}\binom{m}{j}\left(-a^{\dagger}\sin(\theta)\right)^{m-j}\left(b^{\dagger}\cos(\theta)\right)^j.\tag{B.10}$$

Usando os binômios (B.9) e (B.10) em (B.8), obtém-se o estado:

$$\begin{aligned}&e^{-\frac{|\alpha|^2+|\beta|^2}{2}}\sum_{n=0}^{\infty}\sum_{m=0}^{\infty}\sum_{i=0}^{n}\sum_{j=0}^{m}\frac{(\alpha\cos(\theta))^{n-i}}{\sqrt{(n-i)!}}\frac{(-\beta\sin(\theta))^{m-j}}{\sqrt{(m-j)!}}\frac{\left(a^{\dagger}\right)^{n-i}}{\sqrt{(n-i)!}}\frac{\left(a^{\dagger}\right)^{m-j}}{\sqrt{(m-j)!}}\\&\frac{(\alpha\sin(\theta))^{i}}{\sqrt{i!}}\frac{(\beta\sin(\theta))^{j}}{\sqrt{j!}}\frac{\left(b^{\dagger}\right)^{i}}{\sqrt{i!}}\frac{\left(b^{\dagger}\right)^{j}}{\sqrt{j!}}|0\rangle|0\rangle\end{aligned}\tag{B.11}$$

.

Multiplicando, agora, $\frac{\sqrt{[m+n-(j+i)]!}}{\sqrt{[m+n-(j+i)]!}}$ e $\frac{\sqrt{(j+i)!}}{\sqrt{(j+i)!}}$ na expressão (B.11), tem-se:

$$= e^{-\frac{|\alpha|^2+|\beta|^2}{2}} \sum_{n=0}^{\infty} \sum_{m=0}^{\infty} \sum_{i=0}^{n} \sum_{j=0}^{m} \frac{\sqrt{[m+n-(j+i)]!}}{\sqrt{[m+n-(j+i)]!}} \frac{(\alpha\cos(\theta))^{n-i}}{\sqrt{(n-i)!}} \frac{(-\beta\sin(\theta))^{m-j}}{\sqrt{(m-j)!}} \frac{(a^+)^{n-i}}{\sqrt{(n-i)!}} \frac{(a^+)^{m-j}}{\sqrt{(m-j)!}}$$
$$\frac{\sqrt{(j+i)!}}{\sqrt{(j+i)!}} \frac{(\alpha\sin(\theta))^i}{\sqrt{i!}} \frac{(\beta\sin(\theta))^j}{\sqrt{j!}} \frac{(b^\dagger)^i}{\sqrt{i!}} \frac{(b^\dagger)^j}{\sqrt{j!}} |0\rangle|0\rangle \tag{B.12}$$

$$= e^{-\frac{|\alpha|^2+|\beta|^2}{2}} \sum_{n=0}^{\infty} \sum_{m=0}^{\infty} \sum_{i=0}^{n} \sum_{j=0}^{m} \frac{(\alpha\cos(\theta))^{n-i}}{\sqrt{(n-i)!}} \frac{(-\beta sin(\theta))^{m-j}}{\sqrt{(m-j)!}} \frac{\sqrt{[m+n-(j+i)]!}}{\sqrt{(n-i)!}\sqrt{(m-j)!}} |m+n-(j+i)\rangle$$
$$\frac{(\alpha sin(\theta))^i}{\sqrt{i!}} \frac{(\beta sin(\theta))^j}{\sqrt{j!}} \frac{\sqrt{(j+i)!}}{\sqrt{i!}\sqrt{j!}} |j+i\rangle \tag{B.13}$$

.

Pode-se ver que $j+i$ nunca vai ser maior que $m+n$. Fazendo, então, as seguintes mudanças de variáveis

$$m+n-(j+i)=s,\ (j+i)=l \text{ e } n-i=t, \tag{B.14}$$

tem-se uma nova parametrização onde *s, t* e *l* são de variáveis positivas, variando de zero a infinito. As relações ainda implicam em $m-j=s-t$, logo o seguinte rearranjo dos termos da série em função dos novos termos da parametrização é possível:

$$= e^{-\frac{|\alpha|^2+|\beta|^2}{2}} \sum_{s=0}^{\infty} \sum_{l=0}^{\infty} \sum_{t=0}^{s} \sum_{i=0}^{l} \frac{(\alpha\cos(\theta))^t}{\sqrt{t!}} \frac{(-\beta\sin(\theta))^{s-t}}{\sqrt{(s-t)!}} \sqrt{\binom{s}{t}} |s\rangle \sqrt{\binom{l}{i}} \frac{(\alpha\sin(\theta))^i}{\sqrt{i!}} \frac{(\beta\sin(\theta))^j}{\sqrt{(l-i)!}} |l\rangle$$
$$= e^{-\frac{|\alpha|^2+|\beta|^2}{2}} \sum_{s=0}^{\infty} \sum_{l=0}^{\infty} \sum_{t=0}^{s} \sum_{i=0}^{l} \sqrt{s!} \frac{(\alpha\cos(\theta))^t}{t!} \frac{(-\beta\sin(\theta))^{s-t}}{(s-t)!} |s\rangle \sqrt{l!} \frac{(\alpha\sin(\theta))^i}{i!} \frac{(\beta\sin(\theta))^j}{(l-i)!} |l\rangle \tag{B.16}$$

.

Multiplicando (B.16) por $\frac{\sqrt{s!}}{\sqrt{s!}}$ e $\frac{\sqrt{l!}}{\sqrt{l!}}$ para retomarmos ao binômio, tem-se:

$$e^{-\frac{|\alpha|^2+|\beta|^2}{2}} \sum_{s=0}^{\infty} \frac{(\alpha\cos(\theta)-\beta\sin(\theta))^s}{\sqrt{s!}} |s\rangle \sum_{l=0}^{\infty} \frac{(\alpha\sin(\theta)+\beta\cos(\theta))^l}{\sqrt{l!}} |l\rangle. \tag{B.17}$$

Sabendo que:

$$\begin{aligned}&\left(\alpha\cos\left(\theta\right)-\beta\sin\left(\theta\right)\right)\left(\alpha^{*}\cos\left(\theta\right)-\beta^{*}\sin\left(\theta\right)\right)+\left(\alpha\sin\left(\theta\right)+\beta\cos\left(\theta\right)\right)\left(\alpha^{*}\sin\left(\theta\right)+\beta^{*}\cos\left(\theta\right)\right)\\&=\left|\alpha\cos\left(\theta\right)-\beta\sin\left(\theta\right)\right|^{2}+\left|\alpha\sin\left(\theta\right)+\beta\cos\left(\theta\right)\right|^{2}=\left|\alpha\right|^{2}+\left|\beta\right|^{2}\end{aligned} \tag{B.18}$$

A igualdade (B.18) garante a conservação de energia na saída do operador quântico de rotação. A equação (B.17) pode ser re-escrita como:

$$e^{-\frac{\left|\alpha\cos(\theta)-\beta\sin(\theta)\right|^{2}}{2}}\sum_{s=0}^{\infty}\frac{\left(\alpha\cos\left(\theta\right)-\beta\sin\left(\theta\right)\right)^{s}}{\sqrt{s!}}\left|s\right\rangle e^{-\frac{\left|\alpha\cos(\theta)+\beta\sin(\theta)\right|^{2}}{2}}\sum_{l=0}^{\infty}\frac{\left(\alpha\sin\left(\theta\right)+\beta\cos\left(\theta\right)\right)^{l}}{\sqrt{l!}}\left|l\right\rangle. \tag{B.19}$$

.

Portanto, o resultado final é:

$$e^{i\theta\hat{S}_{3}}\left|\alpha\right\rangle\left|\beta\right\rangle=\left|\alpha\cos\left(\theta\right)-\beta\sin\left(\theta\right)\right\rangle\left|\alpha\cos\left(\theta\right)+\beta\sin\left(\theta\right)\right\rangle. \tag{B.20}$$

.

Referências

[1] Simon J. D. Phoenix e Paul D. Townsend, "Quantum Cryptography how to beat the code breakers using quantum mechanics", Contemporary Physics, Vol. 36, nº 3, pp. 165-195, 1995.

[2] Charles H. Bennet, "Quantum Cryptography Using Any Two Nonorthogonal States", Physical Review Letters, Vol. 68, Nº 21, pp. 3121-3124, May 1992.

[3] K. J. Blow e Simon J. D. Phoenix, "On a fundamental theorem of quantum cryptography", Journal of Modern Optics, Vol. 40, nº 1, pp. 33-36, 1993.

[4] G. Barbosa, E. Corndorf, P. Kumar, H. Yuen, " Secure Communication Using Mesoscopic Coherent States ",Phys. Rev. Lett. 90, 227901, 2003.

[5] A. Luis, "Quantum degree of polarisation", Phys. Rev. A, 66, 13806, 2002.

[6] M.A. Nielsen e I.L. Chuang, "Quantum Computation and Quantum Information", Cambridge Univ. Press, Cambridge, 2000.

[7] S. J. Savory e F. P. Payne, "Pulse propagation in Fibers with Polarization-Mode Dispersion", J. of Lightwave Tech., 19, 03, 350, 2001.

[8] G. D. VanWiggeren e R. Roy, "Transmission of linearly polarized light through a single-mode fiber with random fluctuations of birefringence", Applied opt., 38, 18, 3888, 1999.

[9] D. Mahgerefteh e C. R. Menyuk, "Effect of First-Order PMD Compensation on the Statistics of Pulse Broadening in a Fiber with Randomly Varying Birefringence", IEEE Phot. Tech. Lett., 11, 30, 340, 1999.

[10] M. Born, e E. Wolf, "Principles of Optics", 7th ed., Cambridge University Press, Cambridge, England, 1999.

[11] Joseph W. Simmons e Mark J. Guttmann, States, “Waves and Photons: A Modern Introduction to Light”, Addison-Wesley, 1970.

[12] Robson, B. A., “The Theory of Polarisation Phenomena”, Claredon Press, Oxford, 1974.

[13] Chirkin, A. S., Orlov, A. A., e Paraschuk, D. Yu., Quantum Electron., 23, 870, 1993.

[14] Usachev, P., Söderholm, J., Björk, G. e Trifonov, A., “Experimental verification of differences between classical and quantum polarization properties ”, Opt. Commun., 193, 161, 2001.

[15] Andrei B. Klimov, José L. Romero e Luis L. Sánchez-Soto, “A simple quantum model for light depolarization”, xxx.lanl.gov - quant-ph/0406066, 2004.

[16] G. S. Agarwal, J. Lehner e H. Paul, “Optics Communication”, vol 129, pg. 369, 1996.

[17] Prakash, H., e Chandra, N., “Density Operator of Unpolarized Radiation”, Phys. Rev. A, 4, 796, 1971.

[18] Lehner, J., Leonhardt, U., e Paul, H., “Unpolarized light: Classical and quantum states”, Phys. Rev. A, 53, 2727, 1996.

[19] J. C. do Nascimento e R. V. Ramos, “Dynamic of the degree of polarization in a depolarizing channel: theory and experimental results”, Microwave and Optical Technology Letters, vol. 47, nº. 5, 497-500, 2005.

[20] J. Breguet, A. Muller e N. Gisin, "Quantum cryptography with polarized photons in optical fibres: Experimental and Practical Limits", Journal of Modern Optics, Vol. 41, nº 12, pp. 2405-2412, 1994.

[21] J. Breguet, A. Muller e N. Gisin, “Experimental Demonstration of Quantum Cryptography Using Polarized Photons in Optical Fibre over More than 1 km”, Europhys. Lett., 383, 1993.

[22] J. D. Frasson e H. Ilves, “Quantum cryptography using optical fibers”, Appl. Opt., 33, 14, 2949, 1994.

[23] J. D. Frasson e H. Ilves, "Quantum Cryptography using polarization feedback", Jornal of Modern Optics, Vol. 41, nº 12, pp. 2391-2396, 1994.

[24] Simon J. D. Phoenix e Paul D. Townsend, "Quantum Cryptography: how to beat the code breakers using quantum mechanics", Contemporary Physics, Vol. 36, nº 3, pp. 165-195, 1995.

[25] Charles H. Bennet, "Quantum Cryptography Using Any Two Nonorthogonal States", Physical Review Letters, Vol. 68, nº 21, pp. 3121-3124, May 1992.

[26] P. D. Townsend, J. G. Rarity e P. R. Tapster, "Single Photon Interference in 10 km Long Optical Fibre Interferometer", Electronics Letters, Vol. 29, nº 7, pp. 634-635, April 1993.

[27] P. D. Townsend, J. G. Rarity e P. R. Tapster, "Enhanced Single Photon Fringe Visibility in a 10 km-Long Prototype Quantum Cryptography Channel", Electronics Letters, Vol. 29, nº 14, pp. 1291-1293, July 1993.

[28] Paul D. Townsend e I. Thompson, "A quantum key distribution channel based on optical fibre", Journal of Modern Optics, Vol. 41, nº 12, pp. 2425-2433, 1994.

[29] Paul D. Townsend, C. Marand, S. J. D. Phoenix, K. J. Blow e S. M. Barnett, "Secure optical communications systems using quantum cryptography", Phil. Trans. R. Soc. Lond. A, nº 354, pp. 805-817, 1996.

[30] K. J. Gordon, V. Fernandez, P. D. Townsend, e G. S. Buller, “A short wavelength gigahertz clocked fiber-optic quantum key distribution system”, IEEE Journal of Quantum Electronics, vol. 40, nº 7, 900-908, 2004.

[31] K. J. Gordon, V. Fernandez, G. S. Buller , I. Rech, S. D. Cova, e P. D. Townsend, “Quantum key distribution system clocked at 2GHz”, Optics Express, vol. 13, nº. 8, 3015-3020, 2005.

[32] J. C. Bienfang, A. J. Gross, A. Mink, B. J. Hershman, A. Nakassis, X. Tang, R. Lu, D. H. Su, C. W. Clark, C. J. Williams, E. W. Hagley e J. Wen, “Quantum key distribution with 1.25 Gbps clock synchronization”, Optics Express, vol. 12, nº 9, 2011-2016, 2004.

[33] T. B. Pitman, B. C. Jacobs e J. D. Franson, “Experimental Demonstration of a Quantum Circuit using Linear Optics Gates”, Phys. Rev. A 71, 032307, 2005.

[34] F. M. Spedalieri, H. Lee, e J. P. Dowling, “High-fidelity linear optical quantum computing with polarization encoding”,quant-ph/0508113, 2005.

[35] T. C. Ralph, A. G. White, W. J. Munro, e G. J. Milburn, “Simple scheme for efficient linear optics quantum gates”, Phys. Rev. A, 65, 012314, 2001.

[36] P. Kok, W. J. Munro, K. Nemoto, T. C. Ralph, J. P. Downling, e G. J. Milburn,” Review article: Linear optical quantum computing”, quant-ph/0512071, 2005.

[37] G. A. Barbosa, "Parametric Down-Conversion Luminescence: A Fertile Ground in Quantum Optics", Brazilian Journal of Physics, Vol. 25, nº 4, pp. 335-375, December 1995.

[38] Artur K. Ekert, "Quantum Cryptography Based on Bell's Theorem", Physical Review Letters, Vol. 67, nº 6, pp. 661 August 1991.

[39] Artur K. Ekert, John G. Rarity, Paul R. Tapster e G. Massimo Palma, "Practical Quantum Cryptography Based on Two-Photon Interferometry", Physical Review Letters, Vol. 69, nº 9, pp. 1293 August 1992.

[40] P.W. Schor, “Scheme for reducing decoherence in quantum computer memory”, Phys. Rev. A 52 R2493, 1995.

[41] A. Ekert e C. Macchiavello, “Error correction in quantum communication”, Phys. Rev. Lett., 77.2585, arXiv:quant-ph/9602022, 1996.

[42] D. Kalamidas, “Single-photon quantum error rejection and correction with linear optics”, Phys. Lett. A 343, p. 331-335, 2005.

[43] N. Gisin, G. Ribordy, W. Tittel, H. Zbinden,”Quantum cryptography”, Rev. Mod. Phys. 74 145, 2002.

[44] H. Yuen, “KCQ: A New Approach to Quantum Cryptography I. General Principles and Key Generation”, quant-ph/0311061, 2004.

[45] E. Corndorf, G. Barbosa, C. Liang, H. P. Yuen, and P. Kumar, "High-speed data encryption over 25km of fiber by two-mode coherent-state quantum cryptography." Optics Letters, 28: 2040-2042, 2003.

[46] Brito, D.B., Ramos, R.V.,"Passive quantum error correction with linear optics", Physics Letters A, *352, 3, 27, Pg 206-209,* March 2006.

[47] N. Gisin, G. Ribordy, W. Tittel e H. Zbinden,"Quantum cryptography", Rev. Mod. Phys. 74, p. 145, 2002.

[48] J. H. Shapiro e F. N. C. Wong, "Attacking quantum key distribution with single-photon two-qubit quantum logic", Phys. Rev. A, vol. 73, pp. 012315/1-7, 2006.

[49] H. E. Brandt, "Quantum-cryptographic entangling probe", Phys. Rev. A, 71, 042312/1-14, 2005.

[50] C. D. Poole e R. E. Wagner, "Phenomenological approach to polarization dispersion in long single-mode fibers", Etectron. Lett., vol22, pp. 1029-1030, 1986.

[51] A.T. Sornborger e E. D. Stewart. "Higher order methods on computers", Phys. Rev. A60 1956-1965, arXiv:quant-ph/9903055, 1999.