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

MARIA DO SOCORRO RIBEIRO DE OLIVEIRA

CONTRIBUIÇÕES PARA COMUNICAÇÃO E COMPUTAÇÃO QUÂNTICAS: ANÁLISE DO PMD E PDL EM UM SISTEMA DE DQC, GERAÇÃO DE UM ESTADO ENTRELAÇADO DE QUATRO MODOS E UMA PORTA CNOT PARA QUBITS DE ESTADOS COERENTES

FORTALEZA
2013

MARIA DO SOCORRO RIBEIRO DE OLIVEIRA

CONTRIBUIÇÕES PARA COMUNICAÇÃO E COMPUTAÇÃO QUÂNTICAS: ANÁLISE DO PMD E PDL EM UM SISTEMA DE DQC, GERAÇÃO DE UM ESTADO ENTRELAÇADO DE QUATRO MODOS E UMA PORTA CNOT PARA QUBITS DE ESTADOS COERENTES

Dissertação de Mestrado apresentada ao Programa de Pós-Graduação em Engenharia de Teleinformática da Universidade Federal do Ceará, como requisito parcial do Título de Mestre em Engenharia de Teleinformática. Área de concentração: Eletromagnetismo Aplicado.

Orientador: Prof. Dr. João Batista Rosa Silva.

FORTALEZA
2013

Dados Internacionais de Catalogação na Publicação
Universidade Federal do Ceará
Biblioteca de Pós-Graduação em Engenharia - BPGE

O48c Oliveira, Maria do Socorro Ribeiro de.

Contribuições para comunicação e computação quânticas: análise do PMD e PDL em um sistema de DQC, geração de um estado entrelaçado de quatro modos e uma porta CNOT para qubits de estados coerentes / Maria do Socorro Ribeiro de Oliveira. – 2013

60 f. : il. color. , enc. ; 30 cm.

Dissertação (mestrado) – Universidade Federal do Ceará, Centro de Tecnologia, Programa de Pós-Graduação em Engenharia de Teleinformática, Fortaleza, 2013.

Área de concentração: Eletromagnetismo Aplicado.

Orientação: Prof. Dr. João Batista Rosa Silva.

1. Teleinformática. 2. Física quântica. 3. Comunicações ópticas. I. Título.

CDD 621.38

MARIA DO SOCORRO RIBEIRO DE OLIVEIRA

CONTRIBUIÇÕES PARA COMUNICAÇÃO E COMPUTAÇÃO QUÂNTICAS: ANÁLISE DO PMD E PDL EM UM SISTEMA DE DQC, GERAÇÃO DE UM ESTADO ENTRELAÇADO DE QUATRO MODOS E UMA PORTA CNOT PARA QUBITS DE ESTADOS COERENTES

Dissertação submetida à Coordenação do Programa 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.
Área de concentração: Eletromagnetismo Aplicado.

Aprovada em: 22/02/2013.

BANCA EXAMINADORA

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

Prof. Dr. Rubens Viana Ramos
Universidade Federal do Ceará - UFC

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

Prof. Dr. Daniel Barbosa de Brito
Instituto Federal de Educação, Ciência e Tecnologia do Ceará - IFCE

A Deus e a Mãe Santíssima, em primeiro lugar.

A meu pai, Manuel, pela referência de atitudes e a Teresinha, minha mãe, que sempre me incentivou e me mostrou os melhores caminhos na minha vida, in memoriam.

Aos meus irmãos e irmãs, meu grande agradecimento.

Ao meu filho, Wandinho, e ao meu marido, por estarem ao meu lado.

AGRADECIMENTOS

Agradeço-lhe por estar sempre ao meu lado. Você foi o único que me acompanhou e acompanha em todos os momentos. Foi meu amigo, meu pai, porém, o mais importante de tudo, é meu Deus.

Eterno agradecimento ao meu pai, Manoel, de onde tive o exemplo de luta e atitudes e a minha querida mãe, Teresinha, que foi meu berço de amor e proteção em minha vida, apesar de não acompanharem fisicamente minhas conquistas, desejavam sempre as minhas vitórias. Meus irmãos, João, Manoel Filho, Gleide, Íris, Lúcia, Ribeiro, Jânio e Ivanilde, também tiveram coparticipação, pois sempre se preocuparam e me conduziram, mesmo à distância, em minhas trajetórias.

Ao meu filho, Wandinho, pois sacrifiquei alguns bons momentos de sua vida.

Ao meu esposo por aceitar minhas ausências.

Gostaria de um agradecimento, em especial, ao meu orientador professor João Batista por seu grande empenho, suas atitudes de amigo e companheiro, as quais permitiram que eu conseguisse realizar este trabalho.

Ao professor. Rubens, por seu incentivo, orientações e desafios.

À professora Hilma por suas contribuições no trabalho.

Quero agradecer, também, aos demais que fazem parte do grupo GIQ: Keuliane, Davi, Luzeilton, Fátima, Emanuela, Fábio, Glaucionor, Paulo Vinícius, Daniel, Fernando, Daniela, Geovan e Cláudio por sua ajuda em aulas.

"Faça as coisas o mais simples que você puder, porém não se restrinja às mais simples."

(Albert Einstein)

SUMÁRIO

1 INTRODUÇÃO 15

2 CONCEITOS FUNDAMENTAIS 18

2.1 Introdução 18

2.2 Bit Quântico 18

2.2.1 Estado CAT 20

2.3 Principais portas quânticas 21

2.4 Entrelaçamento 23

2.5 Dispositivos ópticos lineares 23

2.6 Canal Quântico 24

2.6.1 Efeitos do PMD e PDL 25

2.7 Protocolo BB84 26

3 ANÁLISE DO IMPACTO DO PMD E PDL EM UM SISTEMA DQC 28

3.1 Introdução 28

3.2 Relação entre PMD e PDL com QBER e taxa de chave segura 28

3.3 Análise de segurança do sistema DQC 30

4 GERADOR DE UM TIPO DE ESTADO ENTRELAÇADO DE QUATRO MODOS PARA QUBITS DE ESTADOS COERENTES 34

4.1 Introdução 34

4.2 Geração de um tipo de estado de quatro modos 35

4.3 Análise da probabilidade de sucesso do gerador 37

5 PROPOSTA DE UMA PORTA CNOT PROBABILÍSTICA PARA QUBITS DE ESTADOS COERENTES 40

5.1 Introdução 40

5.2 Circuito óptico para porta CNOT probabilística 40

5.3 Análise da probabilidade de sucesso e fidelidade 42

6 CONCLUSÕES E PERSPECTIVAS FUTURAS 48

REFERÊNCIAS 50

APÊNDICE A – CÁLCULO DA FIDELIDADE MÉDIA EM FUNÇÃO DOS PARÂMETROS PMD E PDL 56

APÊNDICE B - CÁLCULO DA PROBABILIDADE DE SUCESSO DO GERADOR 58

APÊNDICE C - OPERADOR DE DESLOCAMENTO 60

RESUMO

Este trabalho apresenta contribuições para a área quântica, no âmbito da comunicação e da computação. Na área de comunicação quântica, foram analisados os impactos dos efeitos do PMD e PDL no desempenho de sistemas de distribuição quântica de chaves baseados no protocolo BB84, sob uma rede óptica a fibra. É demonstrada uma expressão analítica da fidelidade média em função dos parâmetros de PMD e PDL, o qual torna possível a análise do comportamento das taxas de erro de bit e de geração de bit seguro de um sistema de comunicação quântica. No campo da computação quântica, são propostos dois sistemas ópticos baseados em óptica linear para qubits de estados coerentes. O primeiro consiste em um gerador probabilístico de um tipo de estado entrelaçado de quatro modos com uma eficiência máxima de 25%. A partir desse estado foi possível propor um segundo sistema que é capaz de realizar uma porta CNOT probabilisticamente. Ambos os sistemas propostos são de implementação factível com a tecnologia fotônica existente, não utilizam portas de um qubit nem teleportação quântica, que são recursos comumente empregados em processamento quântico da informação para estados coerentes.

Palavras-chaves: BB84. PMD. PDL. Estado entrelaçado de quatro modos. Porta CNOT probabilística.

ABSTRACT

This work presents contributions to the quantum communication and in computation fields. In the area of quantum communication, we analyzed the impacts of the effects of PMD and PDL on the performance of a quantum key distribution system based on BB84 protocol in a fiber optic network. It was presented an analytical expression for the average fidelity as a function of the PMD and PDL parameters which makes possible to analyze the behavior of bit error and secure bit generation rates for a quantum communication system. In the field of quantum computing, we proposed two optical systems based on linear optics for coherent state qubits. The first system is a probabilistic generator of a four-mode-type entangled state with a maximum efficiency of 25%. From this it state was possible to propose a second system that is able to perform a probabilistically CNOT gate. Both proposed systems may be implemented with existing photonics technology. They do not use single-qubit gate or quantum teleportation that are commonly used in quantum information processing using coherent states.

Keywords: BB84. PMD. PDL. Four-mode-type entangled state. Probabilistic CNOT gate.

LISTA DE ILUSTRAÇÕES

Figura 2.1 – Esfera de Bloch. 19

Figura 2.2 – Principais portas de um qubit e suas respectivas operações. 22

Figura 2.3 – Representação esquemática da porta CNOT. 23

Figura 2.4 – Representação de um divisor de feixe balanceado (BBS). 24

Figura 2.5 – Sistema de distribuição de chaves quântica simulado com o protocolo BB84. .. 26

Figura 2.6 – Representação das Bases em BB84. 27

Figura 3.1 – QBER para o protocolo BB84, versus o comprimento do canal L com uma PMD de 0,1 ps/km$^{1/2}$ e para uma PDL de 0 dB, 5 dB e 10 dB. 32

Figura 3.2 – Taxa de geração de chave segura para o protocolo BB84, versus o comprimento do canal L, com uma PMD de 0,1 ps/km$^{1/2}$, e uma PDL de 0 dB, 5 dB e 10 dB. 32

Figura 4.1 – Circuito quântico para gerar um estado quatro modos entrelaçado $|\psi\rangle$. 35

Figura 4.2 – Circuito óptico gerador do estado entrelaçado de quatro modos $|\psi\rangle$. 35

Figura 4.3 – Probabilidade de sucesso versus $|\alpha|^2$ para HD's ideais e reais com $\eta = 0.2$ e pd = 10-5. 38

Figura 4.4 – Probabilidade de sucesso em função de $|\alpha|^2$ e η for $p_d = 10^{-5}$. 39

Figura 5.1 – Circuito para geração de um estado quatro modos do tipo entrelaçado $|0100\rangle_{1\text{-}4}$ para qubits de fótons únicos $|\Omega\rangle$. 40

Figura 5.2 – Esquema óptico capaz de desempenhar uma porta CNOT probabilística com qubits de estados coerentes. 41

Figura 5.3 – Probabilidade total de sucesso e da fidelidade total versus $|\alpha|^2$ para um sistema óptico sem perdas e contador de número de fótons ideais. (a) $\theta = \pi/4$ e $\phi = \pi/4$; (b) $\theta = \pi/4$ e $\phi = 2\pi/3$; (c) $\theta = \pi/3$ e $\phi = 2\pi/3$. 46

Figura 5.4 – Probabilidade total de sucesso em função de θ e ϕ para $|\alpha|^2 = 0.25$ e $|\alpha|^2 = 25$. . 46

Figura 5.5 – Fidelidade total em função de θ e ϕ para $|\alpha|^2 = 0.25$ e $|\alpha|^2 = 25$. 47

TABELA

Tabela 1 – As 16 situações possíveis (diferenciados pelo número de fótons n_x registrados e acionamento dos PS's) e o operador de recuperação correspondente necessário para o correto funcionamento da porta CNOT. 45

LISTA DE ABREVIATURAS E SIGLAS

BB84	*Bennett* e *Brassard* – 1984
CD	Dispersão Cromática (*Chromatic Dispersion*)
CP	Controlador de Polarização (*Phase Controller*)
CSQIP	Processamento da Informação Quântica com Estados Coerentes (*Quantum Information Processing with Coherent States*)
DGD	Atraso Diferencial de Grupo (*Differential Group Delay*)
DOP	Grau de Polarização (*Degree of Polarization*)
DQC	Distribuição Quântica de Chaves (*Quantum Key Distribution*)
NLSE	Equação de Schrödinger Não-Linear (*Equation Schrödinger Nonlinear*)
PDL	Perda Dependente da Polarização (*Polarization Dependent Loss*)
PMD	Dispersão por Modo de Polarização (*Polarization mode dispersion)*
PNS	Divisão de Número de Fóton (*Division Photon Number*)
PSD	Densidade Espectral de Potência (*Power Spectral Density*)
PSP	Principal Estado de Polarização (*Principal State of Polarization*)
QBER	Taxa de Erro de Bit Quântico (*Bit Error Rate of Quantum*)
QC	Criptografia Quântica (*Quantum Cryptography*)
QIP	Processamento da Informação Quântica (*Quantum Information Processing*)
SOP	Estado de Polarização (*State of Polarization*)

1 INTRODUÇÃO

> "Na tentativa de julgarmos o sucesso de uma teoria física, poderemos nos questionar sobre dois pontos: (1) Esta é a teoria correta? (2) Esta é a descrição dada pela teoria completa? Assim, apenas no caso em que respostas positivas possam ser dadas a essas duas perguntas, que os conceitos da teoria podem ser considerados satisfatórios" [1].

O processamento quântico da informação é atualmente tratado em países desenvolvidos como uma das tecnologias que deve ser plenamente dominada por quem deseja manter a hegemonia tecnológica e econômica neste novo século. Um desses fatos pode ser verificado pelas quantias gastas por governos e empresas de grande porte da área de telecomunicações e computação, em todo o mundo. E, em particular, esse interesse deve-se ao fato das grandes potencialidades apresentadas pelos sistemas quânticos na solução de problemas complexos.

Porém, apesar de suas potencialidades, arquitetar um computador com processamento totalmente quântico, ainda está por ser elaborado, mesmo em pleno século XXI. E mais, construir portas quânticas confiáveis, que são a base para todo esse sistema, ainda é um desafio [2]. Diversos tipos de tecnologias foram testados, a fim de desenvolver portas quânticas. Entre elas, as que mais se destacaram e apontaram como promissoras, foram a óptica linear e os dispositivos fotônicos [3] – [7], pontos quânticos (*quantum dots*) [8], dispositivos supercondutores [9], [10], semicondutores [11], [12], ressonância magnética nuclear (*nuclear magnetic resonance* – NMR) [13] – [15] e íons aprisionados [16], [17]. Assim, os estudos dessas tecnologias apontam suas vantagens e desvantagens, porém, até o momento, as pesquisas não indicam qual delas é a mais apropriada para a aplicação do processamento quântico no futuro próximo.

Por outro lado, a óptica quântica traz uma grande perspectiva para o Processamento da Informação Quântica (*Quantum Information Processing* – QIP). O desenvolvimento de hardware quântico eficiente para computação é no momento um grande desafio para as pesquisas. A capacidade de implementar uma porta CNOT (*controlled not* – CNOT) com resultados satisfatórios é uma das metas de muitos cientistas, uma vez que, qualquer circuito quântico pode ser construído usando portas de um qubit e CNOTs. Muitas portas quânticas tal como as CNOTs, as com Fase Controlada (*Phase Controlled* – CP), SWAP e *Fredkin*, podem ser implementadas para qubits com codificação de fóton e/ou qubit

codificado com variável contínua [18] (normalmente, a probabilidade de sucesso é muito baixa) usando os modos auxiliares, interferômetro óptico linear passivo, detectores de fótons únicos, contadores de fótons, estados entrelaçados e *feed-forward*, [3], [19] – [39]. Mas a CNOT determinística não foi colocada em prática devido à necessidade de operação não linear [40], [41].

Quanto à comunicação quântica, a Distribuição Quântica de Chaves (DQC), a mais desenvolvida das tecnologias quânticas, permite uma comunicação segura entre usuários de uma rede de comunicações. Ela explora os princípios físicos fundamentais para prover a segurança da informação em meios de comunicações ópticas [42]. Usando fontes de fótons únicos, um espião em potencial, no canal quântico, pode ser descoberto através da Taxa de Erro de Bit Quântico (*Bit Error Rate of Quantum* – QBER).

O objetivo da DQC é estabelecer uma chave secreta entre dois parceiros distantes (Alice e Bob) através de um canal quântico, mesmo sob ataques de um espião (Eva). Uma vez que uma chave secreta comum é estabelecida, a mensagem transmitida entre Alice e Bob será codificada usando protocolos clássicos simétricos de criptografia, cuja segurança é garantida sem restrições ao potencial de Eva, mesmo que a mensagem seja enviada em um canal público clássico autenticado [43]. Atualmente, algumas pesquisas estão direcionadas para o envio de mensagens no próprio canal quântico, o que é chamado de "*Quantum Secure Direct Communication*" [44].

Um problema importante na DQC é o comportamento dos sistemas na presença de perturbações no canal quântico (ex.: o efeito da despolarização, erro de fase, etc.), conectando o transmissor e o receptor [45]. Dois efeitos principais modificam o estado de polarização da luz em fibras ópticas, que são: a perda dependente da polarização (*Polarization Dependent Loss* – PDL) e a dispersão dos modos de polarização (*Polarization Mode Dispersion* – PMD). Trata-se de duas propriedades lineares que são encontradas em enlaces de fibra óptica de longa distância. Esses efeitos podem também estar presentes em componentes ópticos, tais como cristais birrefringentes e polarizadores [46], [47].

Existem, também, dois pontos importantes em relação à distância para a DQC: a geração de fótons únicos e a detecção dos fótons. Assim, têm-se hoje diversas pesquisas por dispositivos que garantam a funcionalidade dos sistemas e cubram esses requisitos [44].

Este trabalho tem como objetivo contribuir para o desenvolvimento tanto da comunicação quanto da computação quântica. No campo da comunicação quântica, foram analisados os impactos dos efeitos da PMD e PDL, em um sistema de DQC baseado em fibra óptica, nas taxas de erro de bit (QBER) e na geração de bit seguro, para o protocolo BB84

[48], [49]. As propostas de um gerador de um tipo de estado de quatro modos entrelaçados e de uma CNOT quântica para qubits de estados coerentes são as contribuições para a computação quântica.

Esta dissertação está dividida em cinco capítulos. No Capítulo 2, são apresentados alguns conceitos importantes para entendimento do trabalho. No Capítulo 3, foram analisados os impactos dos efeitos da PMD e PDL nos sistemas de DQC baseados em uma rede óptica, a fibra para o protocolo BB84. Há, também, uma proposta de um gerador não determinístico de um de tipo de estado entrelaçado de quatro modos para qubits de estados coerentes, bem como uma CNOT probabilística que faz uso daquele estado entrelaçado, ambos usando apenas dispositivos ópticos lineares, que são apresentados, respectivamente, no Capítulo 4 e no Capítulo 5. Por fim, no Capítulo 6, serão apresentadas as conclusões e perspectivas deste trabalho.

2 CONCEITOS FUNDAMENTAIS

2.1 Introdução

Neste capítulo, são apresentados alguns conceitos importantes para auxiliar na compreensão da dissertação. Na Seção 2.2, são apresentadas as definições de qubit codificado na polarização de fótons (únicos ou isolados) e em estados coerentes. Na Seção 2.3, são descritas as principais portas quânticas. Um simples comentário sobre entrelaçamento é visto na Seção 2.4. A descrição do funcionamento dos principais dispositivos ópticos lineares empregados neste trabalho é objeto da Seção 2.5. A Seção 2.6 apresenta uma breve revisão dos efeitos da PMD e PDL presentes em canal quântico de longa distância baseado em fibra óptica. Por fim, uma breve descrição do protocolo BB84 é feita na Seção 2.7.

2.2 Bit Quântico

O bit quântico – qubit é a unidade básica da computação quântica. Em contraste com o sistema clássico, o qubit é uma superposição de estados $|0\rangle$ e $|1\rangle$. Isso significa que esses estados podem ser representados por um vetor em um espaço de Hilbert bidimensional, dados por [19]:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle = \alpha\begin{pmatrix}1\\0\end{pmatrix} + \beta\begin{pmatrix}0\\1\end{pmatrix}, \tag{2.1}$$

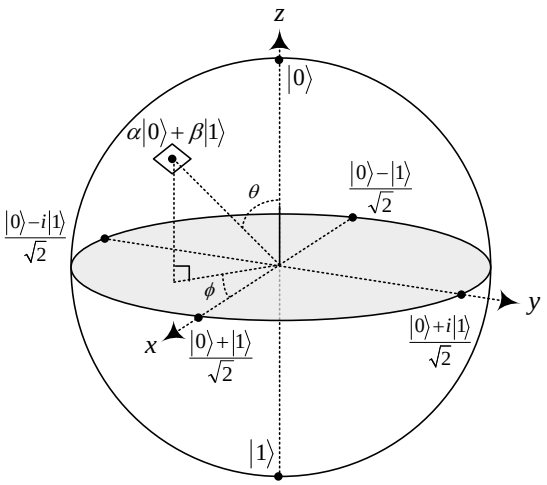
sendo que α e β são números complexos, $|\alpha|^2 + |\beta|^2 = 1$ e $|0\rangle$ e $|1\rangle$ formam uma base ortonormal neste espaço de Hilbert, definindo uma base computacional.

A forma geral do estado puro de um qubit é:

$$|\psi\rangle = \cos\left(\frac{\theta}{2}\right)|0\rangle + e^{j\varphi} sen\left(\frac{\theta}{2}\right)|1\rangle, \tag{2.2}$$

Pode-se, assim, visualizar o estado apresentado em (2.2) na esfera de Bloch, conforme a seguir (FIGURA 2.1). Cada eixo representa uma base existente em um espaço de Hilbert de duas dimensões, e os estados de bases diferentes não são ortogonais entre si [39].

Figura 2.1 – Esfera de Bloch.



Fonte: [50]. Quaisquer dois estados diametralmente opostos formam uma base para descrever um qubit, e quaisquer duas linhas ortogonais que passem pela origem definem duas bases mutuamente não ortogonais.

Atualmente, a representação física mais adotada de um qubit é a polarização do campo eletromagnético de um fóton (horizontal-*H* e vertical-*V*), que se distingue como qubit de polarização [3] – [7]. Neste caso, adota-se a codificação dos qubits lógicos como: $|0\rangle_L = |H\rangle$ e $|1\rangle_L = |V\rangle$. Esse tipo de qubit é de fácil codificação e decodificação, através de placas de meia-onda, quarto de onda e divisores de feixes por polarização, mas é problemático para o transporte em fibras ópticas devido aos efeitos descritos na Seção 2.6.

Outra forma de representação física de qubit em óptica é por meio de estados coerentes. Os estados coerentes são autoestados do operador de aniquilação $\hat{a}$, com autovalor complexo α, isto é, $\hat{a}|\alpha\rangle=\alpha|\alpha\rangle$, e foram introduzidos por R. J. Glauber em 1963 [51]. Eles podem ser escritos na base dos estados de Fock, também chamado de estados de número de fótons, como:

$$|\alpha\rangle = e^{-|\alpha|^2/2}\sum_{n=0}^{\infty}\frac{\alpha^n}{\sqrt{n!}}|n\rangle . \tag{2.3}$$

Em informação quântica, a ortogonalidade entre os dois estados que representam os qubits lógicos é fundamental para a correta distinção das informações. O produto interno entre dois estados coerentes, $|\alpha\rangle$ e $|\beta\rangle$, é dado por:

$$\langle\alpha|\beta\rangle = \exp\left\{\frac{1}{2}\left[2\alpha^*\beta-\left(|\alpha|^2+|\beta|^2\right)\right]\right\} . \tag{2.4}$$

Assim, os qubits lógicos são codificados usando $|0\rangle_L = |-\alpha\rangle$ e $|1\rangle_L = |\alpha\rangle$, sendo α um número real. Esse tipo de codificação é chamado de (–,+) e por meio da equação (2.4), tem-se:

$$\left|\langle\alpha|-\alpha\rangle\right|^2 = e^{-4|\alpha|^2}. \tag{2.5}$$

A falta de ortogonalidade entre os estados $|\alpha\rangle$ e $|-\alpha\rangle$ é um problema para esse tipo de codificação, pois dificulta a distinção dos mesmos. Por isso, exige-se que α seja grande o suficiente para minimizar este problema. A maioria das portas quânticas para esse tipo de qubit requer $\alpha \geq 2$, o qual proporciona uma boa aproximação de ortogonalidade uma vez que $|\langle-\alpha|\alpha\rangle|^2 \leq 1{,}1254\cdot10^{-7}$ [52], para esse valor de α [19], [21], [23]. Também é possível definir os qubits lógicos na base (0, α), $|0\rangle_L = |0\rangle$ (vácuo) e $|1\rangle_L = |2\alpha\rangle$.

2.2.1 Estado CAT

Um ponto interessante da física quântica é a possibilidade de geração macroscópica de superposições quânticas macroscópicas, classicamente distinguíveis. Essa ideia está relacionada com o famoso paradoxo do gato de Schrödinger, onde o gato pode estar vivo ou morto com probabilidades iguais até que a medição seja feita. Na literatura recente apenas a superposição de dois estados coerentes com uma diferença de fase e uma grande amplitude herda esse nome, e é referido como um estado *cat* [53].

O estado cat é definido como uma superposição de dois estados coerentes com fases opostas [19]:

$$\left|\Psi_{\pm}(\alpha)\right\rangle = \frac{1}{\sqrt{N_{\pm}(\alpha)}}\left(\left|-\alpha\right\rangle \pm \left|\alpha\right\rangle\right), \tag{2.6}$$

onde $N_{\pm}(\alpha) = 2 \pm 2e^{-2\alpha^2}$.

Observando que, quando o estado $\left|\Psi_{+}(\alpha)\right\rangle$ é expresso em número de fótons, tem-se:

$$\begin{aligned}\left|\Psi_{+}(\alpha)\right\rangle &= \frac{e^{-\alpha^2/2}}{\sqrt{N_{+}(\alpha)}}\left[\sum_{n=0}^{\infty}\frac{(-\alpha)^n}{\sqrt{n!}}\left|n\right\rangle + \sum_{n=0}^{\infty}\frac{(\alpha)^n}{\sqrt{n!}}\left|n\right\rangle\right] = \frac{e^{-\alpha^2/2}}{\sqrt{N_{+}(\alpha)}}\sum_{n=0}^{\infty}\frac{(\alpha)^n}{\sqrt{n!}}\left[(-1)^n+1\right]\left|n\right\rangle \\ &= \frac{2e^{-\alpha^2/2}}{\sqrt{N_{+}(\alpha)}}\sum_{n=0}^{\infty}\frac{(\alpha)^{2n}}{\sqrt{(2n)!}}\left|n\right\rangle.\end{aligned} \tag{2.7}$$

Enquanto o estado $|\Psi_{-}(\alpha)\rangle$ é descrito como:

$$|\Psi_{-}(\alpha)\rangle = \frac{e^{-\alpha^2/2}}{\sqrt{N_{-}(\alpha)}}\left[\sum_{n=0}^{\infty}\frac{(-\alpha)^n}{\sqrt{n!}}|n\rangle - \sum_{n=0}^{\infty}\frac{(\alpha)^n}{\sqrt{n!}}|n\rangle\right] = \frac{e^{-\alpha^2/2}}{\sqrt{N_{-}(\alpha)}}\sum_{n=0}^{\infty}\frac{(\alpha)^n}{\sqrt{n!}}\left[(-1)^n - 1\right]|n\rangle$$
$$= \frac{2e^{-\alpha^2/2}}{\sqrt{N_{-}(\alpha)}}\sum_{n=0}^{\infty}\frac{(\alpha)^{2n+1}}{\sqrt{(2n+1)!}}|2n+1\rangle \qquad (2.8)$$

A partir das expressões (2.7) e (2.8), pode-se perceber que o $|\Psi_{+}(\alpha)\rangle$ contém somente números pares de fótons e o estado $|\Psi_{-}(\alpha)\rangle$ contém somente números ímpares. Por esta razão, eles podem ser chamados respectivamente de estados cat par e cat ímpar. Nota-se, também, que são estados ortogonais entre si, e que se podem conseguir medidas distintas de acordo com a contagem dos fótons [19].

2.3 Principais portas quânticas

Qualquer porta *U* (2x2) de um qubit de polarização pode ser construída usando-se um rotacionador de polarização entre dois compensadores de fase [54]. Essa transformação é descrita por:

$$U = e^{j\varphi}R_z(\theta_z)R_y(\theta_y)R_z(\theta_z). \qquad (2.9)$$

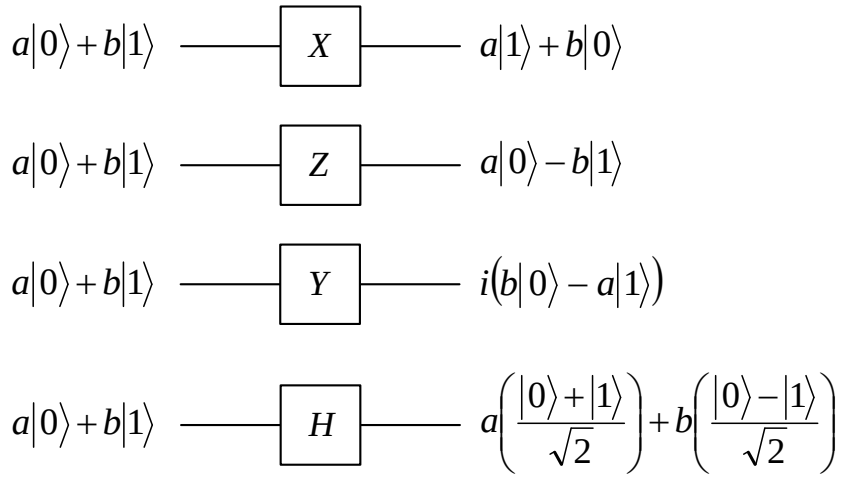
Em (2.9) o operador $R_i(\theta_i) = \exp(j\theta_i\sigma_i)$ (i=x,y,z) representa uma rotação de θ_i em torno do eixo-i da esfera de Bloch. A matriz σ_i é uma das matrizes de Pauli:

$$\sigma_x = \begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix};\ \sigma_y = \begin{bmatrix}0 & -i\\ i & 0\end{bmatrix};\ \sigma_z = \begin{bmatrix}1 & 0\\ 0 & -1\end{bmatrix}. \qquad (2.10)$$

Os operadores σ_x, σ_z e σ_y correspondem, respectivamente, às operações lógicas *X* (inversão de bit – NOT), *Z* (inversão de fase – *phase-flip*) e *Y* (operação combinada de *X* e *Z*), conforme mostradas (FIGURA 2.2). Outra porta de um qubit muito utilizada é a porta Hadamard (*H*), que realiza a seguinte operação: $|0\rangle \rightarrow (|0\rangle + |1\rangle)2^{1/2}$ e $|1\rangle \rightarrow (|0\rangle - |1\rangle)/2^{1/2}$. Essa porta também é mostrada (FIGURA 2.2) e a sua matriz unitária correspondente é [2]:

$$H = \frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}. \qquad (2.11)$$

Figura 2.2 – Principais portas de um qubit e suas respectivas operações.



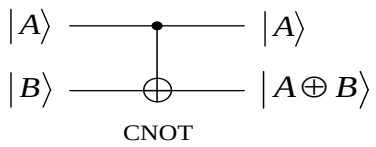
Fonte: [2].

Entre as portas de dois qubits, a mais importante é a CNOT. Trata-se de uma porta NOT controlada por um qubit de controle. A operação NOT será ativada sobre o segundo qubit, denominado de alvo, somente quando o controle for $|1\rangle$. Ou seja, se $|A\rangle = a|0\rangle + b|1\rangle$ e $|B\rangle = c|0\rangle + d|1\rangle$ são, respectivamente, os qubits de controle e alvo, então, a operação realizada pela porta CNOT será $\text{CNOT}|A, B\rangle \rightarrow ac|00\rangle + ad|01\rangle + bc|11\rangle + bd|10\rangle$. Outra maneira de descrever a CNOT é por meio de uma generalização da porta clássica XOR, uma vez que a ação da CNOT pode ser resumida como $\text{CNOT}|A,B\rangle \rightarrow |A, A \oplus B\rangle$. Essa porta tem a seguinte representação matricial:

$$U_{CNOT} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}. \qquad (2.12)$$

Vale ressaltar que qualquer circuito quântico pode ser construído usando somente portas de um qubit e CNOTs [39]. A representação esquemática da porta CNOT é apresentada logo à frente (FIGURA 2.3) [2].

Figura 2.3 – Representação esquemática da porta CNOT.



Fonte: [2].

2.4 Entrelaçamento

O entrelaçamento quântico, proposto por Schrödinger, estudado na mecânica quântica descreve a correlação não local entre sistemas quântico, não explicado pela Mecânica Clássica. O entrelaçamento é atualmente reconhecido como um importante recurso na realização de tarefas tais como, teleportação de estados quânticos, codificação densa, dentre outros.

Estados entrelaçados podem ser criados interagindo dois ou mais sistemas individuais através de uma operação unitária. Propriedades como spin de elétrons ou polarização de fótons, por exemplo, podem ser entrelaçadas [55].

2.5 Dispositivos ópticos lineares

Os principais dispositivos ópticos usados neste trabalho foram: o divisor de feixe balanceado (BBS) e o modulador de fase (PS). O BBS realiza uma função importante na geração de superposição de estados. Sendo $\hat{a}^{\dagger}$ o operador de criação, ter-se-á o operador unitário de um BBS sem perda, definido conforme a seguir:

$$\hat{B} = \exp[\pi(\hat{a}_1\hat{a}_2{}^{\dagger} + \hat{a}_1{}^{\dagger}\hat{a}_2)/4]. \tag{2.13}$$

Assim, quando dois estados coerentes $|\alpha\rangle_1$ e $|\beta\rangle_2$ passam por um BBS, conforme apresentado (FIGURA 2.4), o estado resultante na saída é:

$$|\alpha,\beta\rangle_{1,2} \xrightarrow{BBS} \left|(\alpha-\beta)/\sqrt{2},(\alpha+\beta)/\sqrt{2}\right\rangle_{1,2}. \tag{2.14}$$

O modulador de fase – PS, por sua vez, adiciona uma fase θ ao sinal óptico que o atravessa. O operador unitário correspondente é [19]:

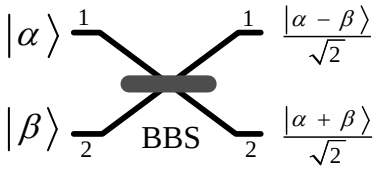
$$\hat{U}(\theta) = \exp\left(j\theta\hat{a}^{\dagger}\hat{a}\right). \tag{2.15}$$

Se o sinal de entrada for $|\alpha\rangle$, na saída do PS o estado será:

$$|\alpha\rangle \xrightarrow{PS} |e^{j\theta}\alpha\rangle . \tag{2.16}$$

Assim, se $\theta = \pi$, o PS funciona, para qubits de estados coerentes, como a porta NOT (X). Essa porta pode ser implementada, para qubit codificado na polarização, por meio de um rotacionador de $\pi/2$ [2].

Figura 2.4 – Representação de um divisor de feixe balanceado (BBS).



Fonte: [2].

2.6 Canal Quântico

Todos os sistemas quânticos são sistemas abertos mesmo que a interação com o meio seja muito pequena. Em uma rede óptica, apesar da fraca interação dos qubits fotônicos (sistemas quânticos) em uma fibra óptica (canal), a descoerência atuará na atenuação, despolarização e/ou dispersão dos qubits quando se propagam na fibra óptica.

A taxa de absorção, ou perda, tem seu valor mínimo no comprimento de onda de 1550 nm em fibras ópticas. Para fibra monomodo, a perda é calculada por $10^{-\lambda L/10}$ onde L é o comprimento da fibra (distância de transmissão), λ representa a atenuação da fibra em torno de 2 a 3 dB/km para a primeira janela de transmissão (880 nm), 0,35 dB/km para a segunda (1310 nm) e 0,20 dB/km para a terceira janela (1550 nm). As fibras comerciais são bons meios para transportar qubits fotônicos, mas longe de serem perfeitos, por causa de três principais efeitos: a Dispersão do Modo de Polarização (*Polarization mode dispersion* – PMD), a Perda Dependente da Polarização (*Polarization Dependent Loss* – PDL) e a Dispersão Cromática (*Chromatic Dispersion* – CD) [2]. O primeiro é devido à variação aleatória da birrefringência da fibra óptica ao longo do tempo e do espaço, levando à despolarização da luz ou mesmo à quebra do pulso portador de informação em dois outros. Enquanto o efeito de PDL tende a polarizar parcialmente a luz uma vez que é um polarizador

parcial, porém diminui a intensidade da luz ao longo da fibra causando perda da potência [44]. Já a CD causa o efeito de descoerência para informação codificada no tempo, ou seja, o qubit de *time-bin*, devido à dispersão temporal dos pulsos de luz [50].

A distribuição quântica de chaves tem por trás todo um processo que se baseia no uso de fóton único. Infelizmente, esses estados são difíceis de produzir experimentalmente. Hoje em dia, implementações práticas dependem de pulsos de laser atenuados ou pares de fótons entrelaçados, em que ambos os fótons e os números de pares de fótons de distribuição obedecem à estatística de Poisson. Nos dois casos mencionados, há uma pequena probabilidade de gerar mais de um fóton ou um par de fótons ao mesmo tempo. Pequenas frações destes multifótons podem ter consequências importantes sobre a segurança da chave [56]. Na próxima seção, ter-se-á um breve resumo sobre as características e parâmetros da fibra óptica relacionada ao trabalho.

2.6.1 Efeitos do PMD e PDL

O que caracteriza a polarização da luz é a distribuição de sua energia em dois eixos (estados) ortogonais, denominados de Estados Principais de Polarização (*Principal State of Polarization* – PSP) [48].

A degeneração natural dos modos ortogonais polarizados não acontece somente para uma fibra ideal monomodo tendo o núcleo como um cilindro perfeito com diâmetro uniforme. Fibras reais exibem variações consideráveis na forma do seu núcleo ao longo de seu comprimento. Elas também podem passar por tensões não uniformes quando, por exemplo, a simetria cilíndrica da fibra é quebrada. Assim, a fibra adquire birrefringência [48].

Em fibras monomodo convencionais, a birrefringência não é constante ao longo da fibra, e sim, muda aleatoriamente, por causa das variações na forma do núcleo (elíptica em vez de circular) devido à tensão anisotrópica que age no núcleo, onde atua em ambos na magnitude e direção. Como resultado, a luz lançada na fibra com polarização linear, rapidamente adquire um estado de polarização arbitrário. Além do mais, diferentes componentes de frequência de um pulso adquirem diferentes estados de polarização, resultando no alargamento do pulso. Esse fenômeno é chamado de Dispersão dos Modos de Polarização e torna-se um fator limitante para sistemas de comunicações ópticas operando em elevadas taxas de bit. Devido à PMD, os modos de polarização ortogonais propagam-se com velocidades diferentes resultando em um atraso entre os modos. Esse atraso é chamado de Atraso Diferencial de Grupo (*Differential Group Delay* – DGD). O valor médio desses atrasos caracteriza o efeito PMD. De acordo com o DGD e com a modulação utilizada, é possível que

ocorra uma redução no Grau de Polarização (*Degree of Polarization* – DOP), o que é indesejável, devido ao espalhamento dos pulsos na fibra [48], [57].

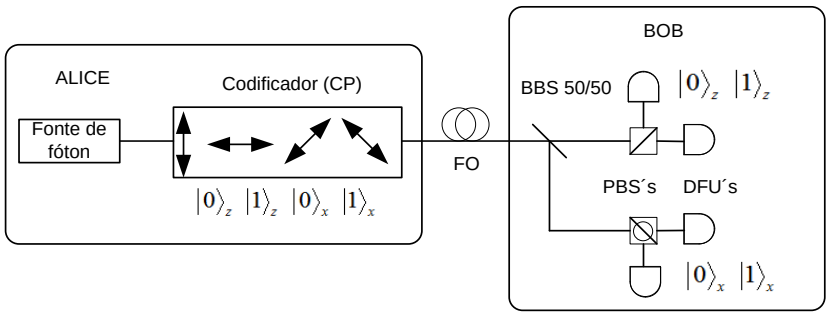
Perdas na transmissão por fibra, geralmente, dependem do Estado de Polarização (*State of Polarization* – SOP) do sinal que se propaga por ela. Essa dependência é conhecida como Perda Dependente da Polarização. Mesmo as fibras de sílica possuem um PDL relativamente pequeno, entretanto, o sinal passa por uma variedade de componentes ópticos como isoladores, moduladores, amplificadores, filtros, e acopladores onde a maioria deles exibe perdas (ou ganho no caso de amplificadores ópticos), na qual a magnitude depende do SOP do sinal [47].

Além do mais, a combinação entre PDL e PMD não leva somente a grandes variações aleatórias na potência do sinal, mas também à distorção do sinal que afeta invariavelmente, o desempenho de todos os sistemas ópticos de longa distância [46], [47].

2.7 Protocolo BB84

Nesta Seção, apresentar-se-á o funcionamento do primeiro protocolo DQC, publicado por *Bennett* e *Brassard* em 1984 e, portanto, chamado BB84 [44]. O funcionamento desse protocolo (FIGURA 2.5) é descrito com base no sistema de DQC para qubits codificados na polarização da luz conforme mostrado mais a frente (FIGURA 2.6) [58].

Figura 2.5 – Sistema de distribuição de chaves quântica simulado com o protocolo BB84.

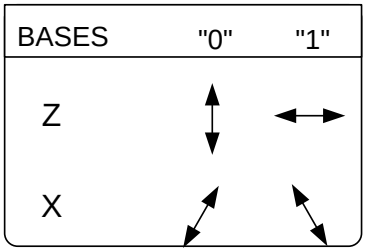


Fonte: [58]. Codificador de Polarização – CP, Divisor de feixe balanceado – BBS, Divisor de feixe por polarização – PBS, Detector de fóton único – DFU.

No protocolo BB84, Alice codifica uma sequência aleatória de bits em uma sequência de qubits baseados na polarização de fótons únicos e envia para Bob por meio de um canal quântico (fibra óptica – FO). Para isso, ela utiliza um Codificador de Polarização –

CP como codificador para formar quatro estados quânticos que são divididos em duas bases, *Z* e *X*, conforme apresentado a seguir (FIGURA 2.6):

Figura 2.6 – Representação das Bases em BB84.



Fonte: [59].

A base *Z* é constituída pelos estados $|0\rangle_z = |\updownarrow\rangle$ (polarização vertical) e $|1\rangle_z = |\leftrightarrow\rangle$ (polarização horizontal) para os bits 0 e 1, respectivamente. A base *X* é formada pelos qubits $|0\rangle_x = |\nearrow\rangle$ (polarização +45º) e $|1\rangle_x = |\nwarrow\rangle$ (polarização – 45º) que correspondem aos bits 0 e 1, respectivamente. Os estados que compõem cada base são ortogonais.

Na sequência, Bob mede a polarização de cada fóton enviado por Alice e armazena o valor medido sequencialmente. Para isso, ele usa um divisor de feixe balanceado (BBS) para escolher aleatoriamente a base de medição, uma vez que ele não sabe qual foi a base que Alice utilizou para o qubit [58]. Ao finalizar a transmissão, Bob revela para Alice, através de um canal público, a base que ele usou para medir cada qubit, mas sem revelar o resultado da medição. Ambos descartam os bits, cujas bases de codificação e medição divergem. Os bits restantes formam uma chave bruta comum a ambos. Essa etapa é chamada de “peneiramento”.

Na etapa seguinte conhecida por reconciliação de chaves, Alice e Bob escolhem um subconjunto da chave bruta e o compara através do canal público, o objetivo é avaliar a taxa de erro da comunicação. Desde que, Eva (espiã) tenha interferido no sistema, ela provocará um erro com probabilidade de 25% (vinte e cinco por cento) por fóton enviado na comunicação direta entre Alice e Bob. Assim, a partir dessas condições, a chave será descartada e o processo reiniciado.

Caso, após a avaliação do processo de reconciliação, não seja detectada a presença de Eva no subconjunto, os erros existentes são removidos de forma clássica, reduzindo o tamanho do subconjunto, o qual formará a chave segura. Ainda com o objetivo de aumentar a privacidade, Alice e Bob aplicam uma função *Hash* nas chaves. A chave, finalmente, após todo esse processo de correção de erro e amplificação de privacidade, estará pronta para codificar uma mensagem.

3 ANÁLISE DO IMPACTO DO PMD E PDL EM UM SISTEMA DQC

3.1 Introdução

Este capítulo analisa o desempenho de um sistema de distribuição quântica de chaves baseado no protocolo BB84 com estados de polarização de pulsos de luz Gaussianos em um canal quântico, cujos efeitos da PMD e PDL estão presentes. Também é apresentada uma expressão analítica da fidelidade média em função dos parâmetros da PMD e da PDL presentes em enlace de fibra óptica, bem como a taxa de erro de bit quântico (QBER).

Ter-se-á, na Seção 3.2, o formalismo matemático que relaciona a PMD e PDL com a fidelidade média. Na Seção 3.3, é apresentado o estudo da QBER e a taxa de geração de chave segura para estados de polarização, tendo como base o protocolo BB84. Nesse ponto, serão apresentados os resultados do comportamento da QBER e da taxa de geração de chave segura em função do comprimento do canal (enlace óptico).

3.2 Relação entre PMD e PDL com QBER e taxa de chave segura

A descrição quântica da polarização é semelhante à descrição clássica, sendo conveniente o uso do formalismo de vetores de Jones de duas dimensões. Os pares de polarização ortogonais – linear (horizontal/vertical), diagonal (+45º/–45º) e circular (direita/esquerda) – são descritos, respectivamente, pelos autovetores das matrizes de Pauli, (conforme já descritas em (2.10)) [46], [60]. Nesse caso, qualquer estado de polarização pode ser descrito como uma superposição de um par de autovetores com coeficientes complexos.

O efeito da PMD em uma onda monocromática de frequência ω separa os autovetores de σ_z por uma birrefringência b (DGD) o qual é representado pelo operador [60]:

$$U_{PMD} = e^{j\omega b\sigma_z/2} = \cos\left(\frac{\omega b}{2}\right)\mathbf{1} + j\,\mathrm{sen}\left(\frac{\omega b}{2}\right)\sigma_z. \tag{3.1}$$

Esse operador unitário U_{PMD} descreve uma rotação global do estado de polarização em torno do eixo z da esfera de Poincaré.

Quanto ao efeito da PDL, os estados mais e menos atenuados, que são sempre ortogonais, podem ser escritos como autoestados de $\sigma_n = \hat{n}\cdot\vec{\sigma}$, sendo que a direção $\hat{n}$ não tem, *a priori*, nenhuma relação com a direção $\hat{z}$ do eixo de birrefringência. Negligenciando a atenuação global, a PDL pode ser representada pelo operador não unitário [60]:

$$U_{PDL} = e^{\alpha\sigma_n/2} = \cosh\left(\frac{\alpha}{2}\right)\mathbf{1} + \operatorname{senh}\left(\frac{\alpha}{2}\right)\sigma_n, \tag{3.2}$$

onde α é o coeficiente de perda da PDL.

Uma vez que qualquer rede óptica pode ser modelada por um elemento de PMD seguido por um elemento PDL [61], o operador geral será o produto dos operadores de PMD e PDL, ou seja, U_{PDL} x U_{PMD}. Para simplificar o modelo da rede óptica, os parâmetros α, b e $\hat{n}$ são considerados independentes da frequência ω.

O estado de entrada, no domínio do tempo, é um pulso de luz Gaussiano de tempo de coerência t_c e de frequência central ω_0, preparado em um estado de polarização puro $|\psi_0\rangle$ [60]:

$$\left|\Psi_{in}\right\rangle = \mathcal{A}e^{-\frac{t^2}{4t_c^2}}e^{-j\omega_0 t} \otimes \left(\varepsilon\left|H\right\rangle + \lambda\left|V\right\rangle\right) = g\left(t\right)\otimes\left|\psi_0\right\rangle, \tag{3.3}$$

onde $\mathcal{A} = \left(\sqrt{2\pi}t_c\right)^{-1/2}$ e $|g(t)|^2$ é a distribuição de probabilidade. Assim, o estado de saída da rede óptica, no domínio da frequência, é dado por:

$$\left|\Psi_{out}\right\rangle = U_{PDL}U_{PMD}\left|\Psi_{in}\right\rangle_{\omega} = N\left(\varepsilon e^{\alpha/2}e^{j\omega b/2}\left|H\right\rangle + \lambda e^{-\alpha/2}e^{-j\omega b/2}\left|V\right\rangle\right)G\left(\omega\right), \tag{3.4}$$

sendo $N = [(|\varepsilon|^2 e^{\alpha} + |\lambda|^2 e^{-\alpha})]^{-1/2}$ a constante de normalização, $G(\omega)$ a transformada de Fourier de $g(t)$ e $|\Psi_{in}\rangle_{\omega} = G(\omega)|\psi_0\rangle$. Seja $g(t)$ um processo estocástico, a fidelidade média $\mathcal{F}$ considerando (3.1) e (3.2) é [48]:

$$\mathcal{F} = \lim_{t_c\to\infty}\frac{1}{2\pi t_c}\int_{-\infty}^{+\infty} E\left\{\left|\left\langle\Psi_{in}\left(\omega\right)\middle|\Psi_{out}\left(\omega\right)\right\rangle\right|\right\}d\omega = N\left(\left|\varepsilon\right|^2 e^{\alpha/2}\mathcal{R}(b/2) + \left|\lambda\right|^2 e^{-\alpha/2}\mathcal{R}(-b/2)\right), \tag{3.5}$$

onde $\mathcal{R}(\cdot)$ é a função de autocorrelação de $g(t)e^{j\omega_0 t}$ e considerando que α varia entre $-0{,}1 \leq \alpha \geq 0{,}1$, para mais detalhes, consultar resultados obtidos no Apêndice A.

É fato que, na ausência de efeitos não lineares, um pulso Gaussiano permanece Gaussiano durante a propagação, mas a largura do pulso muda com a distância devido à dispersão cromática presente na fibra óptica [62]. A CD faz com que os variados comprimentos de onda viajem com velocidades ligeiramente diferentes, conduzindo, assim, a uma expansão temporal incoerente do pulso de luz. Isso pode ser problemático quando pulsos subsequentes começam a se sobrepor. Esse efeito altera o tempo de coerência (diferença de

fase constante) do pulso óptico de entrada e a largura do pulso de saída τ, após propagar uma distância L, o qual pode ser expresso em função dos parâmetros da fibra, sem *chirp*, como [47]:

$$\tau(L) = t_c \sqrt{1 + \left(\frac{L}{L_D}\right)^2}, \tag{3.6}$$

onde $L_D = t_c^2 / |\beta_2|$ é o comprimento de dispersão, e $\beta_2 = D\lambda^2/(2\pi c)$ é o parâmetro de dispersão de segunda ordem da fibra, sendo D o parâmetro de dispersão com um valor típico de 17 ps/(km-nm) em fibras de telecomunicações padrão, λ é o comprimento de onda de operação (1550 nm) e c é a velocidade da luz no vácuo.

3.3 Análise de segurança do sistema DQC

Pesquisas recentes analisaram o comportamento da taxa de geração de chave segura e do QBER para o protocolo BB84 e SARG04 na presença de despolarização no canal quântico. O resultado experimental mostra que o protocolo SARG04 é mais suscetível ao efeito de despolarização no canal quântico que o BB84 [44], [59], [63].

Atualmente, a despolarização do canal é analisada por meio do parâmetro da visibilidade do sistema óptico de comunicação [44], [49], [64], sem uma compreensão detalhada da contribuição dos efeitos da PMD e PDL no desempenho de um sistema DQC. Vários estudos foram realizados quanto aos efeitos da PMD e da PDL em redes de comunicação óptica clássica [57], [65] – [70]. No melhor do conhecimento que se tem na área, nenhum trabalho analisou o impacto da PMD e da PDL em um sistema DQC. É fato que uma compreensão mais precisa desses efeitos propiciará o desenvolvimento de sistemas DQC mais eficientes e de maiores alcances.

Portanto, neste capítulo será analisado analiticamente o comportamento da QBER e da taxa de geração de chaves em um sistema DQC baseado no protocolo BB84 na presença da PMD e PDL.

Será visto, inicialmente, as considerações de segurança relevantes para o protocolo BB84 em DQC para a situação onde o espião (Eva) não está presente, ou seja, os erros são devidos a um canal realístico.

Considerando as imperfeições dos dispositivos que compõem uma rede óptica, a taxa de geração de chave é dada por [49], [71], [72]:

$$r \geq R_1 S_1\left(Q_1\right) - R_\mu h\left(Q_\mu\right), \tag{3.7}$$

onde R_1, R_μ, Q_1 e Q_μ são parâmetros relacionados à chave bruta que podem ser estimados por Alice e Bob: sendo a taxa total de detecção $R_\mu = \sum_n R_n$, no qual R_n é a taxa de detecção de pulsos quando Alice envia n fótons por pulso; $Q_\mu = \sum_n R_n Q_n / R_\mu$ é a taxa total de erro quântico (QBER) para uma taxa de erro Q_n correspondente ao envio de n fótons por pulso pela Alice; $S_1 = 1 - h\left(Q_1\right)$ e $h\left(x\right) = -x log_2\left(x\right) - (1-x) log_2(1-x)$, é a entropia binária. Os parâmetros R_μ, e Q_μ para o protocolo BB84, são respectivamente, dados por [49]:

$$\begin{aligned} R_\mu &= \frac{1}{2}\left(1 - \bar{p}_d^2 e^{-\mu\eta}\right), \\ Q_\mu &= \frac{1}{4R_\mu}\left[1 + \bar{p}_d\left(e^{-\mu\mathcal{F}\eta} - e^{-\mu(1-\mathcal{F})\eta}\right) - \bar{p}_d^2 e^{-\mu\eta}\right], \end{aligned} \tag{3.8}$$

com $\bar{p}_d = 1 - p_d$ e p_d a probabilidade de contagem de escuro dos detectores de Bob, $\mathcal{F}$ a fidelidade, $\eta = \eta_{\text{det}} \cdot 10^{-\alpha_{fo} L/10}$ a eficiência geral de detecção da rede óptica, sendo o comprimento da fibra óptica que separa Alice e Bob é dado por L (km), no qual apresenta um coeficiente de atenuação α_{fo} (dB/km) e uma eficiência dos detectores de Bob de η_{det}. O limite inferior de (3.7) pode ser obtido a partir de [49]:

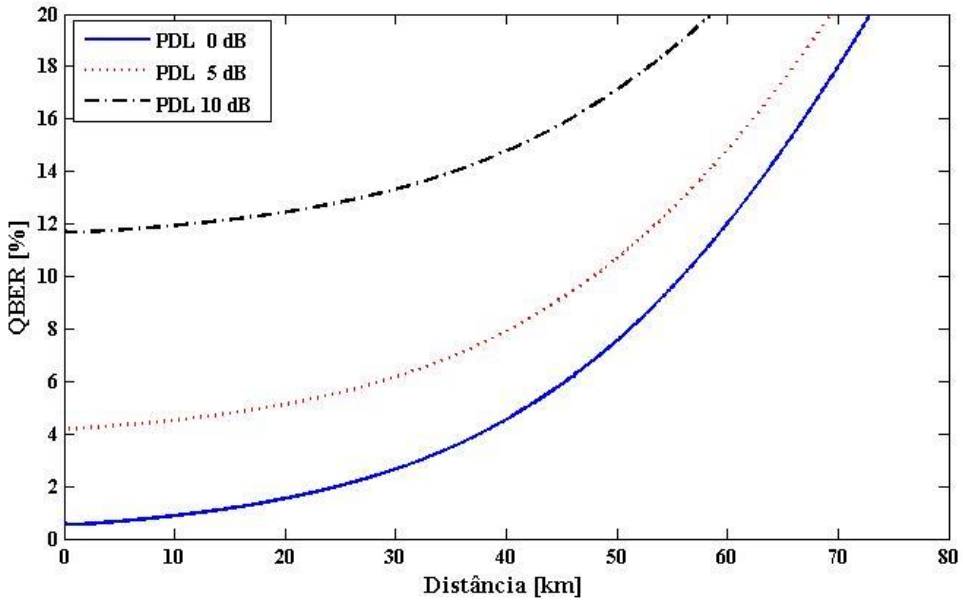
$$r \geq R_1^{\min}\left[1 - h\left(Q_1^{\max}\right)\right] - R_\mu h\left(Q_\mu\right), \tag{3.9}$$

onde $R_1^{\min} = R_\mu - \frac{1}{2}\sum_{n\geq 2} p_n$,

sendo $R_1^{\min} \leq 0$, $R_1 = 0$,então, o limite inferior de r é negativo, isto é, Alice e Bob devem abortar o protocolo. Caso $R_1^{\min} > 0$, $Q_1^{\max} = \min\left(R_\mu Q_\mu / R_1^{\min}, 1/2\right)$.

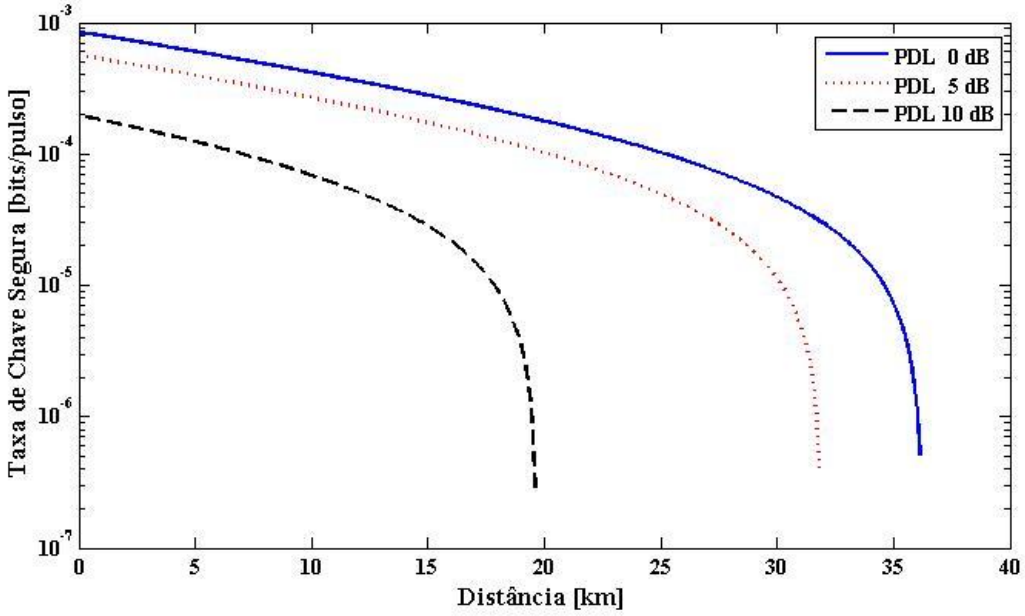
Com o propósito de analisar o efeito da PMD e PDL na taxa de erro (QBER) e na taxa de geração de chave segura para um sistema de distribuição quântica de chave baseado no protocolo BB84, foram traçadas as curvas a partir de (3.8) e (3.9) com valores de PDL de 0 dB, 5 dB e 10 dB em um canal quântico composto por uma fibra óptica monomodo em 1550 nm, um parâmetro de PMD de D_p = 0,1 ps/(km)$^{1/2}$, uma dispersão cromática de 17 ps/(km-nm) e um coeficiente de atenuação α_{fo} = 0,25 dB/km. Foi considerada uma DGD média dado por $b = \langle DGD \rangle = D_p[8L/(3\pi)]^{1/2}$ [47]. Os demais parâmetros são os mesmos usados em [49].
O comportamento da QBER e taxa de geração de chave segura em função do comprimento do canal são apresentados a seguir (FIGURAS 3.1 e 3.2):

Figura 3.1 – QBER para o protocolo BB84, versus o comprimento do canal *L* com uma PMD de 0,1 ps/km$^{1/2}$ e para uma PDL de 0 dB, 5 dB e 10 dB.



Fonte: Elaborada pela autora.

Figura 3.2 – Taxa de geração de chave segura para o protocolo BB84, versus o comprimento do canal *L*, com uma PMD de 0,1 ps/km$^{1/2}$, e uma PDL de 0 dB, 5 dB e 10 dB.



Fonte: Elaborada pela autora.

É percebido no gráfico da QBER e da Taxa de Geração de Chave Segura (FIGURAS 3.1 e 3.2) que a PMD e a PDL degradam o desempenho do sistema à medida que o comprimento do enlace cresce. Para a PDL (FIGURA 3.2) em 0 dB o comportamento de *r* é idêntico ao apresentado em [49].

Como já observado em sistema de comunicação óptica clássica, os efeitos do PMD e PDL degradam o desempenho de um sistema DQC. Sendo assim, é verificado que a taxa de geração de chave, no sistema analisado, decresce à medida que o DGD e PDL aumentam. Portanto, em sistema de comunicação de longa distância, esses efeitos não podem ser negligenciados e sua compreensão mais detalhada propiciará o desenvolvimento de sistemas DQC mais eficientes e de maiores alcances.

4 GERADOR DE UM TIPO DE ESTADO ENTRELAÇADO DE QUATRO MODOS PARA QUBITS DE ESTADOS COERENTES

4.1 Introdução

Os sistemas ópticos demonstram ser uma tecnologia de fácil manipulação e a partir de dispositivos já existentes, podem ser facilmente definidos novos circuitos que apresentam bons resultados para a informação quântica. As principais vantagens são: a geração de estados entrelaçados por meio de conversão paramétrica descendente, a construção de portas CNOT probabilísticas com dispositivos ópticos comuns e a fácil implementação de porta de um qubit [6], [55], [56], [73], [74]. As desvantagens são: a necessidade de um sistema para gerar um único fóton, um canal que seja capaz de transmitir informação com perdas muito baixas e esquemas de detecção eficientes.

Uma alternativa para qubits de fótons únicos é a ideia de codificação de informação quântica em variáveis contínuas de campos multifótons [18]. Isso levou a uma série de propostas para a realização de computação quântica [21], [22], [75], incluindo a implementação de qubit usando superposição de estados coerentes [19], [21], [23]. Até agora, essas aplicações com qubit de estados coerentes não tiveram muito sucesso, principalmente devido a: (1) os protocolos quânticos existentes que utilizam qubits de estados coerentes requerem contadores de fótons; (2) implementação da porta Z, conforme mostrado na seção 2.3, requerer um procedimento de teleportação que pode falhar; e (3) a produção de superposição de estados coerentes se apresenta como uma tarefa tecnicamente difícil [55], [76] – [80].

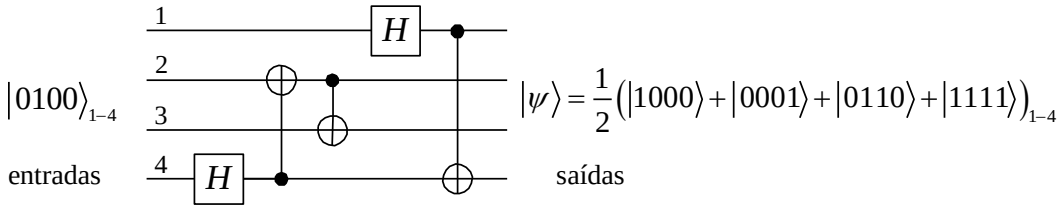
A seguir será proposto um sistema óptico capaz de gerar um tipo de estado entrelaçado de quatro modos para qubit de estado coerente, sem a necessidade de utilização de dispositivos de contagem de fótons. Essa prática apresenta um avanço nas implementações dessa área, onde alguns autores utilizam outros métodos [81] – [85], incluindo o uso de teleportação [86] – [88].

Neste Capítulo, será visto na Seção 4.2, um sistema óptico para geração probabilística de um estado entrelaçado de quatro modos para qubits de estados coerentes e na Seção 4.3, a análise da eficiência do gerador de entrelaçamento.

4.2 Geração de um tipo de estado de quatro modos

O estado entrelaçado de quatro modos proposto é $|\psi\rangle$ = ($|1000\rangle$ + $|0001\rangle$ + $|0110\rangle$ + $|1111\rangle$) /2**.** Esse estado pode ser obtido pelo circuito quântico mostrado a seguir (FIGURA 4.1), cujo estado de entrada é $|0100\rangle_{1\text{-}4}$. Esse circuito quântico é formado por duas portas de Hadamard e três portas CNOT.

Figura 4.1 – Circuito quântico para gerar um estado quatro modos entrelaçado $|\psi\rangle$.



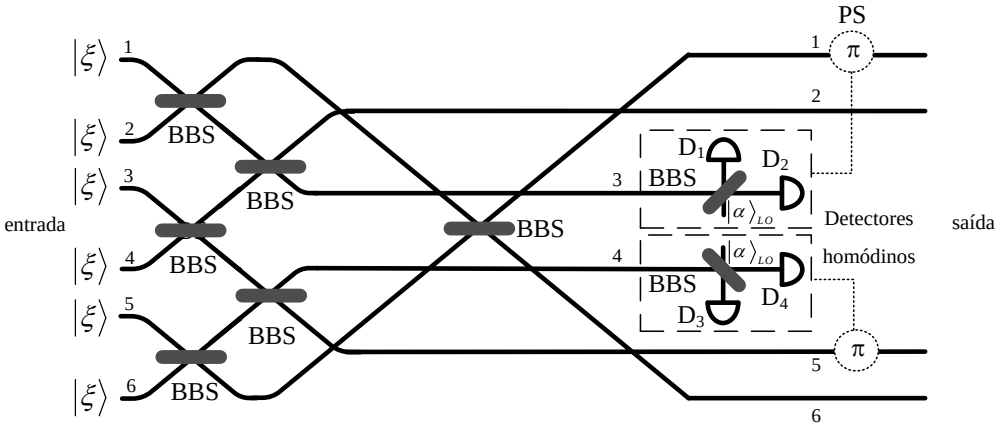
Fonte: Elaborada pela Autora.

O estado $|\psi\rangle$ para qubits de estados coerente conforme descrito na Seção 2.2 é dado por:

$$|\psi\rangle = N\left(|\alpha,-\alpha,-\alpha,-\alpha\rangle + |-\alpha,-\alpha,-\alpha,\alpha\rangle + |-\alpha,\alpha,\alpha,-\alpha\rangle + |\alpha,\alpha,\alpha,\alpha\rangle\right), \tag{4.1}$$

onde N = {2 [1+ exp(–4$|\alpha|^2$) + 2exp(–6$|\alpha|^2$)] $^{1/2}$}$^{-1}$ é a constante de normalização. O circuito óptico capaz de gerar o estado quântico em (4.1) é apresentado a seguir (FIGURA 4.2):

Figura 4.2 – Circuito óptico gerador do estado entrelaçado de quatro modos $|\psi\rangle$.



Fonte: Elaborada pela Autora.

O estado de entrada $|\Psi_{in}\rangle$ é formado por seis estados iguais a $|\xi\rangle = N_\xi(|-\alpha\rangle+|\alpha\rangle)$, em que N_ξ = {2 [1+ exp(–2$|\alpha|^2$)]} $^{-1/2}$ é a constante de normalização. O circuito mostrado

anteriormente (FIGURA 4.2) é composto de divisores de feixe balanceados e moduladores de fase, que funcionam como a porta *X* quanto ativados, conforme descritos na Seção 2.5, e de sistemas de Detecção Homódina – HD, mais detalhes sobre a HD ver referência [19]. Se considerar o estado de entrada como $|\Psi_{in}\rangle = |\xi\rangle^{\otimes 6}$, então, depois de alguns cálculos, pode-se encontrar o seguinte estado de saída antes da detecção homódina:

$$\left|\Psi_{\det}\right\rangle = \frac{N_\xi^6}{N}\left(\left|\psi_1\right\rangle + \left|\psi_2\right\rangle + \left|\psi_3\right\rangle + \left|\psi_4\right\rangle\right) + \frac{N_\xi^6}{N_u}\left|\psi_u\right\rangle, \tag{4.2}$$

onde:

$$\begin{aligned}\left|\psi_1\right\rangle &= \left|\psi\right\rangle_{1256}\left|-\alpha,-\alpha\right\rangle_{34} \\ &= N\left(\left|\alpha,-\alpha,-\alpha,-\alpha\right\rangle + \left|-\alpha,-\alpha,-\alpha,\alpha\right\rangle + \left|-\alpha,\alpha,\alpha,-\alpha\right\rangle + \left|\alpha,\alpha,\alpha,\alpha\right\rangle\right)_{1256}\left|-\alpha,-\alpha\right\rangle_{34}\end{aligned} \tag{4.3}$$

$$\left|\psi_2\right\rangle = \left(I\otimes I\otimes X\otimes I\left|\psi\right\rangle\right)\left|-\alpha,\alpha\right\rangle \tag{4.4}$$

$$\left|\psi_3\right\rangle = \left(X\otimes I\otimes X\otimes I\left|\psi\right\rangle\right)\left|\alpha,-\alpha\right\rangle \tag{4.5}$$

$$\left|\psi_4\right\rangle = \left(X\otimes I\otimes I\otimes I\left|\psi\right\rangle\right)\left|\alpha,\alpha\right\rangle \tag{4.6}$$

$$\begin{aligned}\left|\psi_u\right\rangle = N_u\big(&\left|\varnothing,-\alpha,-2\alpha,\varnothing\right\rangle\left|-\alpha,\varnothing\right\rangle + \left|\varnothing,-\alpha,\varnothing,\varnothing\right\rangle\left|-\alpha,-2\alpha\right\rangle + \cdots \\ &\left|\varnothing,\alpha,\varnothing,\varnothing\right\rangle\left|\alpha,2\alpha\right\rangle + \left|\varnothing,\alpha,2\alpha,\varnothing\right\rangle\left|\alpha,\varnothing\right\rangle\big)_{125634}\end{aligned} \tag{4.7}$$

na qual $N_u = \left\{16e^{-3|\alpha|^2}\cosh\left(|\alpha|^2\right)\sqrt{3\left[1-2\cosh^2\left(|\alpha|^2\right)+4\cosh^4\left(|\alpha|^2\right)\right]}\right\}^{-1}$ é uma constante de normalização.

Em (4.7), $|\psi_u\rangle$ contém as situações em que a detecção acontece em ambos os detectores, D_1 e D_2 e/ou $|D_3$ e $D_4|$. Nesse caso, o circuito falha ($|\varnothing\rangle$ é o estado de vácuo). Da equação (4.3) pode-se também notar que, quando se mede $|-\alpha,-\alpha\rangle$ nos detectores homódinos, nos modos 3 e 4, respectivamente, a saída é $|\psi\rangle$ dada em (4.1), então, as portas *X* são desabilitadas. Por outro lado, se o resultado da medição for $|-\alpha,\alpha\rangle$, então, a porta *X* no modo 5 é ativada, a fim de corrigir o estado de saída, de acordo com (4.4). Se a medição dos HD's indicarem $|\alpha, -\alpha\rangle$, ambas as portas *X* são ativadas, conforme (4.5). Quando a medição dos HD's indicar $|\alpha,\alpha\rangle$, deve ser ativado somente a porta *X* no modo 2 para se obter, na saída do circuito óptico (FIGURA 4.2), o estado (4.1).

4.3 Análise da probabilidade de sucesso do gerador

O elemento crítico desse sistema é o detector homódino, devido ao estado local $|\alpha\rangle_{LO}$ (oscilador local) uma vez que cada um dos osciladores locais $|\alpha\rangle_{LO}$ deverá ter a mesma amplitude dos estados de entrada, e deverá estar sincronizado com os estados nos modos 3 e 4, respectivamente. Uma boa revisão sobre a eficiência da detecção homódina pode ser encontrada em [19], [20], [76] – [80], [82], [89]. Note em (4.2), que a probabilidade de sucesso do sistema (FIGURA 4.3) é 1/4 para $\langle -\alpha\,|\alpha\rangle = 0$, caso sejam utilizados detectores homódinos ideais. No entanto, para $\delta = \langle -\alpha\,|\alpha\rangle = \exp(-2\alpha^2) \neq 0$, a probabilidade de sucesso do gerador é dada pela probabilidade condicional $p_{succ} = p_{1001}\langle\Psi_{det}|\rho_1|\Psi_{det}\rangle + p_{1010}\langle\Psi_{det}|\rho_2|\Psi_{det}\rangle + p_{0101}\langle\Psi_{det}|\rho_3|\Psi_{det}\rangle + p_{0110}\langle\Psi_{det}|\rho_4|\Psi_{det}\rangle$, na qual, por exemplo, p_{1010} é a probabilidade de se ter um clique, nenhum clique, um clique e nenhum clique nos detectores D_1, D_2, D_3 e D_4, respectivamente, e ρ_i é a matriz de densidade do estado $|\psi_i\rangle$. Portanto, a probabilidade de sucesso é:

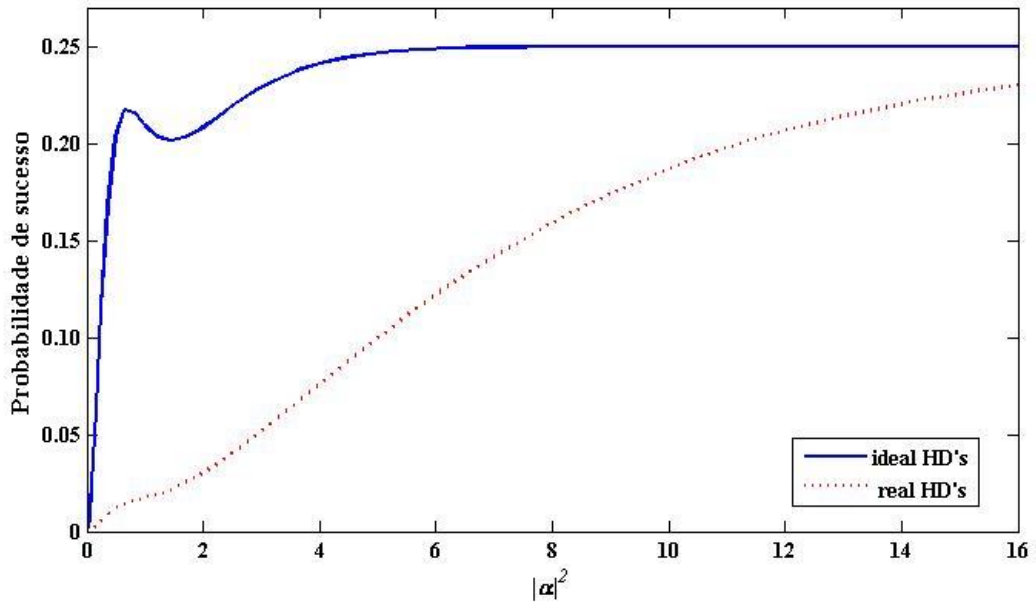
$$p_{succ} = \frac{\left(1-e^{-|\alpha|^2}\right)^2 \cdot \left(1+e^{-2|\alpha|^2}\right)^6}{4\cdot\left(1+e^{-4|\alpha|^2}+2e^{-6|\alpha|^2}\right)}. \tag{4.8}$$

Se considerarmos detectores reais com eficiência quântica η e probabilidade de contagem de escuro p_{dark}. Então, a probabilidade de sucesso real, p_{real}, será dada por:

$$p_{real} = \frac{\left(1-p_{dark}\right)^2\left[1-e^{-|\alpha|^2\eta}\left(1-p_{dark}\right)\right]^2 \cdot \left(1+e^{-2|\alpha|^2}\right)^6}{4\cdot\left(1+e^{-4|\alpha|^2}+2e^{-6|\alpha|^2}\right)}. \tag{4.9}$$

No gráfico a seguir (FIGURA 4.3), pode-se observar a relação entre as probabilidades de sucesso, dadas em (4.8) e (4.9), e o número médio de fótons $|\alpha|^2$ para HD's ideais e reais. Os valores utilizados para a eficiência quântica η e probabilidade de contagem escuro p_{dark} foram de 0,2 e 10^{-5}, respectivamente [55]. Como pode ser observado no gráfico da probabilidade de sucesso em função de α (FIGURA 4.4), para grandes valores de $|\alpha|^2$, o desempenho do gerador de entrelaçamento é maior, com probabilidade de sucesso máxima igual a 1/4. No Apêndice B, apresentam-se mais detalhes sobre os cálculos da Probabilidade.

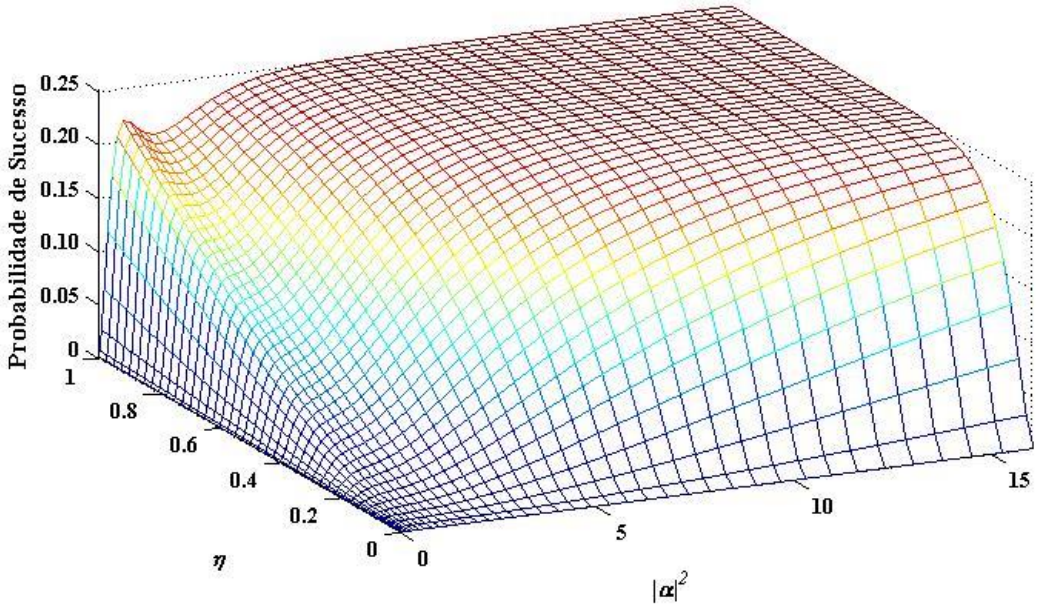
Figura 4.3. Probabilidade de sucesso versus $|\alpha|^2$ para HD's ideais e reais com $\eta = 0.2$ e $p_d = 10^{-5}$.



Fonte: Elaborada pela autora.

As curvas apresentadas (FIGURA 4.4) mostram o comportamento da probabilidade de sucesso em função do número médio de fótons $|\alpha|^2$ e da eficiência quântica η dos detectores de fótons para um valor fixo de probabilidade de contagem de escuro $p_d = 10^{-5}$. Nota-se que a ineficiência dos detectores de fótons não afeta a qualidade da geração do estado entrelaçado (4.1), mas pode diminuir a probabilidade de sucesso em obtê-lo quando considerar um sistema óptico com perdas.

Figura 4.4 – Probabilidade de sucesso em função de $|\alpha|^2$ e η for $p_d = 10^{-5}$.



Fonte: Elaborada pela autora.

5 PROPOSTA DE UMA PORTA CNOT PROBABILÍSTICA PARA QUBITS DE ESTADOS COERENTES

5.1 Introdução

Apresentar-se-á uma nova proposta para a obtenção probabilística de uma porta CNOT para qubits de estados coerentes usando entrelaçado em quatro modos [90], que pode ser obtido a partir do gerador apresentado no Capítulo 4.

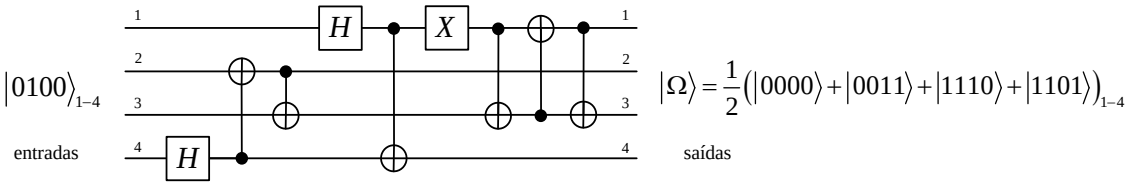
Este capítulo está dividido em duas seções. A Seção 5.2 apresenta-se o circuito óptico proposto que implementa a porta CNOT probabilisticamente para qubits de estados coerentes e a Seção 5.3 traz a análise de sucesso e de fidelidade da porta CNOT proposta na seção anterior.

5.2 Circuito óptico para porta CNOT probabilística

Objetiva-se desenvolver uma porta CNOT onde os estados $|C\rangle = a|0\rangle + b|1\rangle$ e $|T\rangle = c|0\rangle + d|1\rangle$ são os qubits de controle e alvo, respectivamente. Em CSQIP, os estados $|C\rangle$ e $|T\rangle$ são: $|C\rangle = N_c(a|-\alpha\rangle + b|\alpha\rangle)$ e $|T\rangle = N_t(c|-\alpha\rangle + d|\alpha\rangle)$, sendo $N_c = [1+2\cdot\mathcal{R}e\{a^*b\}\cdot\exp(-2|\alpha|^2)]^{-1/2}$ e $N_t = [1+2\cdot\mathcal{R}e\{c^*d\}\cdot\exp(-2|\alpha|^2)]^{-1/2}$ as constantes de normalização.

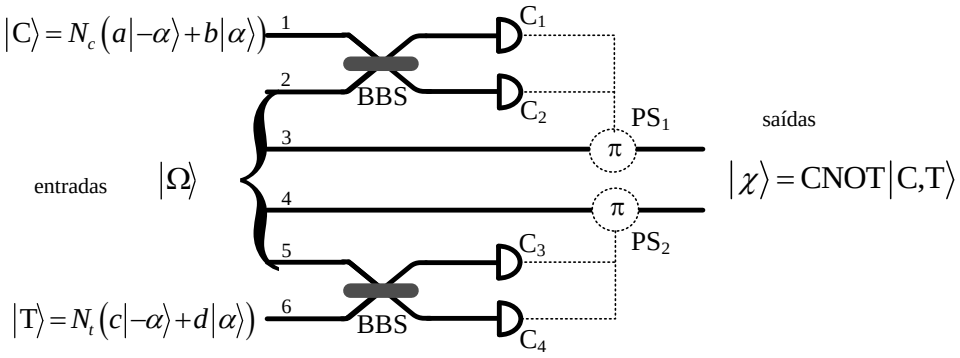
O circuito óptico proposto, capaz de realizar a função da porta CNOT, probabilisticamente é mostrado a seguir (FIGURA 5.2). O estado $|\Omega\rangle$ é um estado entrelaçado de quatro modos e que é dado por $|\Omega\rangle = N_\Omega\cdot(|-\alpha,-\alpha,-\alpha,-\alpha\rangle + |-\alpha,-\alpha,\alpha,\alpha\rangle + |\alpha,\alpha,\alpha,-\alpha\rangle + |\alpha,\alpha,-\alpha,\alpha\rangle)$, sendo $N_\Omega = \{4\cdot[1 + \exp(-4|\alpha|^2) + 2\cdot\exp(-6|\alpha|^2)]\}^{-1/2}$. Esse estado pode ser gerado por um circuito quântico apresentado logo à frente (FIGURA 5.1) e pode ser implementado a partir do esquema óptico não determinístico [91], proposto no Capítulo 4, com probabilidade de sucesso de 1/4.

Figura 5.1 – Circuito para geração de um estado quatro modos do tipo entrelaçado $|0100\rangle_{1\text{-}4}$ para qubits de fótons únicos $|\Omega\rangle$.



Fonte: Elaborada pela autora.

Figura 5.2 – Esquema óptico capaz de desempenhar uma porta CNOT probabilística com qubits de estados coerentes.



Fonte: Elaborada pela autora.

No esquema anterior (FIGURA 5.2), BBS, PS e C são, respectivamente, divisores de feixe balanceado, moduladores de fase e contadores de fóton. Conforme descrito no Capítulo 2, o PS funciona como uma porta NOT ou *X* em CSQIP se $\theta = \pi$. No modo 1 tem-se o qubit de controle $|C\rangle$, no modo 6 tem-se o modo de qubit alvo $|T\rangle$ e os modos 2 a 5 correspondem ao recurso auxiliar $|\Omega\rangle$. Antes dos contadores de fóton, o estado $|\psi\rangle$, resultante da evolução do estado de entrada $|C\rangle_1 \otimes |\Omega\rangle_{2\text{-}5} \otimes |T\rangle_6$ através do sistema óptico, é dado por:

$$\begin{aligned}|\psi\rangle = N\Big[& ac\Big(\big|0,-\sqrt{2}\alpha,-\alpha,-\alpha,0,-\sqrt{2}\alpha\big\rangle + \big|0,-\sqrt{2}\alpha-\alpha,\alpha,\sqrt{2}\alpha,0\big\rangle + \big|-\sqrt{2}\alpha,0,\alpha,\alpha,0,-\sqrt{2}\alpha\big\rangle + \big|-\sqrt{2}\alpha,0,\alpha,-\alpha,\sqrt{2}\alpha,0\big\rangle\Big) + \\ & ad\Big(\big|0,-\sqrt{2}\alpha,-\alpha,-\alpha,-\sqrt{2}\alpha,0\big\rangle + \big|0,-\sqrt{2}\alpha-\alpha,\alpha,0,\sqrt{2}\alpha\big\rangle + \big|-\sqrt{2}\alpha,0,\alpha,\alpha,-\sqrt{2}\alpha,0\big\rangle + \big|-\sqrt{2}\alpha,0,\alpha,-\alpha,0,\sqrt{2}\alpha\big\rangle\Big) + \\ & bc\Big(\big|\sqrt{2}\alpha,0,-\alpha,-\alpha,0,-\sqrt{2}\alpha\big\rangle + \big|\sqrt{2}\alpha,0,-\alpha,\alpha,\sqrt{2}\alpha,0\big\rangle + \big|0,\sqrt{2}\alpha,\alpha,\alpha,0,-\sqrt{2}\alpha\big\rangle + \big|0,\sqrt{2}\alpha,\alpha,-\alpha,\sqrt{2}\alpha,0\big\rangle\Big) + \\ & bd\Big(\big|\sqrt{2}\alpha,0,-\alpha,-\alpha,-\sqrt{2}\alpha,0\big\rangle + \big|\sqrt{2}\alpha,0,-\alpha,\alpha,0,\sqrt{2}\alpha\big\rangle + \big|0,\sqrt{2}\alpha,\alpha,\alpha,-\sqrt{2}\alpha,0\big\rangle + \big|0,\sqrt{2}\alpha,\alpha,-\alpha,0,\sqrt{2}\alpha\big\rangle\Big)\Big],\end{aligned} \tag{5.1}$$

onde $N = N_c\, N_\Omega\, N_t$. Quando o contador de fóton C_x registrar n_x fótons, será obtido um dos seguintes estados no modo 3 e 4:

$$\begin{aligned}|\chi\rangle_{3,4} &= {}_{1,2,5,6}\langle 0,n_2,0,n_4\,|\psi\rangle_{1-6} \simeq \\ & ac(-1)^{n_2+n_4}\,|-\alpha,-\alpha\rangle + ad(-1)^{n_2}\,|-\alpha,\alpha\rangle + bc(-1)^{n_4}\,|\alpha,\alpha\rangle + bd\,|\alpha,-\alpha\rangle,\end{aligned} \tag{5.2}$$

$$\begin{aligned}|\chi\rangle_{3,4} &= {}_{1,2,5,6}\langle n_1,0,n_3,0\,|\psi\rangle_{1-6} \simeq \\ & ac(-1)^{n_1}\,|\alpha,-\alpha\rangle + ad(-1)^{n_1+n_3}\,|\alpha,\alpha\rangle + bc\,|-\alpha,\alpha\rangle + bd(-1)^{n_3}\,|-\alpha,-\alpha\rangle,\end{aligned} \tag{5.3}$$

$$\begin{aligned}|\chi\rangle_{3,4} &= {}_{1,2,5,6}\langle 0,n_2,n_3,0\,|\psi\rangle_{1-6} \simeq \\ & ac(-1)^{n_2}\,|-\alpha,\alpha\rangle + ad(-1)^{n_2+n_3}\,|-\alpha,-\alpha\rangle + bc\,|\alpha,-\alpha\rangle + bd(-1)^{n_3}\,|\alpha,\alpha\rangle,\end{aligned} \tag{5.4}$$

$$|\chi\rangle_{3,4} = {}_{1,2,5,6}\langle n_1, 0, 0, n_4 \,|\, \psi\rangle_{1-6} \simeq$$
$$ac(-1)^{n_1+n_4}\,|\,\alpha,\alpha\rangle + ad(-1)^{n_1}\,|\,\alpha,-\alpha\rangle + bc(-1)^{n_4} bc\,|\,-\alpha,-\alpha\rangle + bd\,|\,-\alpha,\alpha\rangle. \quad (5.5)$$

Em (5.2), observa-se que o contador de fótons C_1 e C_3 registraram ambos zero fóton e os contadores C_2 e C_4 detectaram um número não nulo de fótons, n_2 e n_4, respectivamente. Uma análise similar pode ser feita em (5.3) – (5.5). Assim, o circuito óptico mostrado na Fig. 14 funcionará corretamente se o estado de saída for igual a $|\lambda\rangle = \text{CNOT}|C,T\rangle = N_\lambda(ac|-\alpha,-\alpha\rangle + ad|-\alpha,\alpha\rangle + bc|\alpha,\alpha\rangle + bd|\alpha,-\alpha\rangle)$ ou a um estado que possa ser convertido em $|\lambda\rangle$ por meio de operadores unitários (portas de um qubit, conforme descrito no Capítulo 2), com $N_\lambda = \{1+2\cdot[\mathcal{R}e\{c^*d\}\,(1+2\mathcal{R}e\{a^*b\}) + \mathcal{R}e\{a^*b\}\,\exp(-2|\alpha|^2)]\,\exp(-2|\alpha|^2)\}^{-1/2}$.

Portanto, o sistema óptico funcionará corretamente quando se mede nos contadores de fótons correspondentes, uma das seguintes situações mutuamente exclusivas:

(*i*) $n_1 = n_3 = 0$, ambos n_2 e n_4 forem pares e ambos PS's devem ser desabilitados;
(*ii*) $n_2 = n_4 = 0$, ambos n_1 e n_3 forem pares e somente o PS_1 deve ser ativado;
(*iii*) $n_1 = n_4 = 0$, ambos n_2 e n_3 forem pares e somente o PS_2 deve ser ativado;
(*iv*) $n_2 = n_3 = 0$, ambos n_1 e n_4 forem pares e ambos PS's devem ser ativados.

5.3 Análise da probabilidade de sucesso e fidelidade

Nesta seção, será analisada a probabilidade de sucesso da porta CNOT proposta, considerando cada uma das quatro situações listadas na seção anterior. Para simplificar, assume-se que *a*, *b*, *c*, *d* e α são reais. Então, a probabilidade de sucesso para a situação (*i*), $p_i = |{}_{1,2,5,6}\langle 0,n_2,0,n_4|\psi\rangle_{1\text{-}6}|^2$, é dada por:

$$p_i = \frac{|N|^2}{4|N_\lambda|^2}(1-e^{-2\alpha^2})^2. \quad (5.6)$$

Pode ser verificado em (5.6), que dependendo de α, a probabilidade de um evento bem sucedido é 1/16. O mesmo resultado é obtido para as outras situações ($p = p_i = p_{ii} = p_{iii} = p_{iv}$). Portanto, a probabilidade de sucesso é 1/4.

Um operador de deslocamento apropriado é usado nos casos em que a porta CNOT falha, realizando uma operação chamada de *near-faithful*, isto é, a fidelidade do estado colapsado pode ser quase 1 para um grande valor de $|\alpha|^2$, conforme mostrado no Apêndice C. Supondo que em (5.2) n_2 e n_4 sejam ímpares, resultar-se-á em um estado:

$$|\phi_1\rangle = N_1\left(ac\,|-\alpha,-\alpha\rangle - ad\,|-\alpha,\alpha\rangle - bc\,|\alpha,\alpha\rangle + bd\,|\alpha,-\alpha\rangle\right),$$
$$N_1 = \left\{1-2\left[cd\left(1-2ab\right)+abe^{-2|\alpha|^2}\right]e^{-2|\alpha|^2}\right\}^{-1/2}. \tag{5.7}$$

O estado (5.7) não é igual a $|\lambda\rangle$ e nem pode ser convertido nele por um operador unitário, assim, sua fidelidade será menor que 1. Portanto, pode-se aplicar um operador de deslocamento $\hat{D}_2(\beta) = \exp\left(\beta\hat{a}_2^{\dagger} - \beta^*\hat{a}_2\right)$ no modo 2 em (5.7) para aumentar a fidelidade do estado colapsado. Se $\beta = -j\pi/(4\alpha)$, o estado obtido é:

$$|\phi_1'\rangle = \hat{D}_2\left(-\frac{j\pi}{4\alpha}\right)|\phi_1\rangle = N_1 e^{j\pi/4}\left(ac\left|-\alpha,-\frac{j\pi}{4\alpha}-\alpha\right\rangle + jad\left|-\alpha,-\frac{j\pi}{4\alpha}+\alpha\right\rangle + jbc\left|\alpha,-\frac{j\pi}{4\alpha}+\alpha\right\rangle + bd\left|\alpha,-\frac{j\pi}{4\alpha}-\alpha\right\rangle\right), \tag{5.8}$$

e a fidelidade do estado em (5.8) em relação ao estado desejado $|\lambda\rangle$ é:

$$F_1' = \left|\langle\phi_1'|\lambda\rangle\right| = \left|N_\lambda\right|\cdot\left|N_1\right|\cdot e^{-\pi^2/\left(32|\alpha|^2\right)}\left(1+4\cdot abcd\cdot e^{-2|\alpha|^2}\right). \tag{5.9}$$

Analisando (5.9), observa-se que a fidelidade tende a 1 para um grande valor de $|\alpha|^2$ e a probabilidade de sucesso neste caso é:

$$p_1' = \frac{|N|^2}{4|N_1|^2}(1-e^{-2\alpha^2})^2. \tag{5.10}$$

Agora, supondo que em (5.2) n_2 e n_4, respectivamente, são valores par e ímpar, resultando no seguinte estado na saída, mostrado no circuito da porta CNOT (FIGURA 5.2):

$$|\phi_2\rangle = N_2\left(-ac\,|-\alpha,-\alpha\rangle + ad\,|-\alpha,\alpha\rangle - bc\,|\alpha,\alpha\rangle + bd\,|\alpha,-\alpha\rangle\right),$$
$$N_2 = \left\{1-2\left[cd\left(1+2ab\right)-abe^{-2|\alpha|^2}\right]e^{-2|\alpha|^2}\right\}^{-1/2}. \tag{5.11}$$

Se aplicarmos o operador de deslocamento $\hat{D}(\beta)$ em ambos os modos de (5.11), o estado obtido será dado por:

$$|\phi_2'\rangle = \hat{D}_1\left(-\frac{j\pi}{4\alpha}\right)\otimes\hat{D}_2\left(-\frac{j\pi}{4\alpha}\right)|\phi_2\rangle =$$
$$N_2\left(-jac\left|-\frac{j\pi}{4\alpha}-\alpha,-\frac{j\pi}{4\alpha}-\alpha\right\rangle + ad\left|-\frac{j\pi}{4\alpha}-\alpha,-\frac{j\pi}{4\alpha}+\alpha\right\rangle + jbc\left|-\frac{j\pi}{4\alpha}+\alpha,-\frac{j\pi}{4\alpha}+\alpha\right\rangle + bd\left|-\frac{j\pi}{4\alpha}+\alpha,-\frac{j\pi}{4\alpha}-\alpha\right\rangle\right). \tag{5.12}$$

A fidelidade e a probabilidade de sucesso, neste caso, respectivamente, serão:

$$F_2' = \left|\langle \phi_2' | \lambda \rangle\right| = \left|N_\lambda\right| \cdot \left|N_2\right| e^{-\pi^2/\left(16|\alpha|^2\right)} \left(1 + 2\left(d^2 - c^2\right) ab \cdot e^{-4|\alpha|^2}\right), \tag{5.13}$$

$$p_2' = \frac{\left|N\right|^2}{4\left|N_2\right|^2} (1 - e^{-2\alpha^2})^2. \tag{5.14}$$

Para o caso em que n_2 e n_4 são ímpar e par, respectivamente, o estado projetado com o operador de deslocamento aplicado no modo 1 de (5.2) é dado por:

$$\begin{aligned} \left|\phi_3'\right\rangle &= -N_3 \left(ac \left| -\frac{j\pi}{4\alpha} - \alpha, -\alpha \right\rangle + ad \left| -\frac{j\pi}{4\alpha} - \alpha, \alpha \right\rangle + jbc \left| -\frac{j\pi}{4\alpha} + \alpha, +\alpha \right\rangle + jbd \left| -\frac{j\pi}{4\alpha} + \alpha, -\alpha \right\rangle \right), \\ N_3 &= \left\{ 1 + 2\left[cd\left(1 - 2ab\right) - abe^{-2|\alpha|^2} \right] e^{-2|\alpha|^2} \right\}^{-1/2}. \end{aligned} \tag{5.15}$$

A fidelidade e a probabilidade de sucesso para (5.15) serão, respectivamente:

$$F_3' = \left|\langle \phi_3' | \lambda \rangle\right| = \left|N_\lambda\right| \cdot \left|N_3\right| e^{-\pi^2/\left(32|\alpha|^2\right)} \cdot \left(1 + 2cd \cdot e^{-2|\alpha|^2}\right), \tag{5.16}$$

$$p_3' = \frac{\left|N\right|^2}{4\left|N_3\right|^2} (1 - e^{-2\alpha^2})^2. \tag{5.17}$$

A Tabela 1 mostra todas as 16 situações possíveis onde a CNOT proposta é eficiente e as operações de correções que serão realizadas, dependendo do número de fótons registrados. Portanto, a probabilidade total de sucesso e a fidelidade total do sistema óptico, respectivamente, são:

$$p_T = 4\left(p_1 + p_1' + p_2' + p_3' \right), \tag{5.18}$$

$$F_T = 4\left(p_1 \cdot 1 + p_1' \cdot F_1' + p_2' \cdot F_2' + p_3' \cdot F_3' \right). \tag{5.19}$$

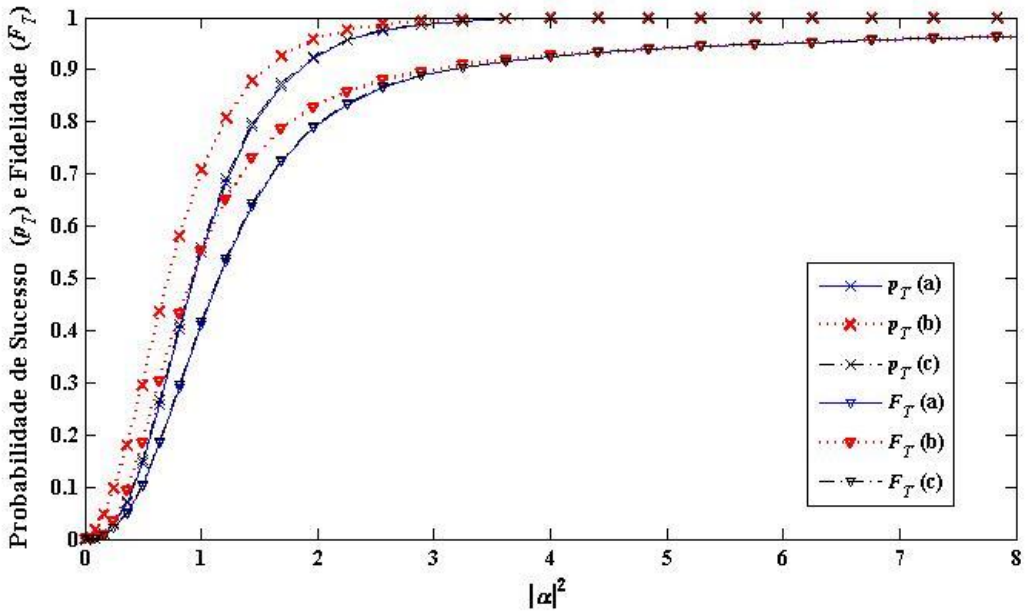
Tabela 1 – As 16 situações possíveis (diferenciados pelo número de fótons n_x registrados e acionamento dos PS's) e o operador de recuperação correspondente necessário para o correto funcionamento da porta CNOT.

Situações possíveis				Estado Colapsado	Modulador de Fase		Operador de Recuperação	Fidelidade	Probabilidade de Sucesso
n_1	n_2	n_3	n_4		PS_1	PS_2			
0	par	0	par	Eq. (5.2)	off	off	$I \otimes I$	1	Eq. (5.6)
0	par	0	ímpar	Eq. (5.2)	off	off	$\hat{D}(\beta) \otimes \hat{D}(\beta)$	Eq. (5.13)	Eq. (5.14)
0	ímpar	0	par	Eq. (5.2)	off	off	$\hat{D}(\beta) \otimes I$	Eq.(5.16)	Eq. (5.17)
0	ímpar	0	ímpar	Eq. (5.2)	off	off	$I \otimes \hat{D}(\beta)$	Eq. (5.9)	Eq. (5.10)
par	0	par	0	Eq. (5.3)	on	off	$I \otimes I$	1	Eq. (5.6)
par	0	ímpar	0	Eq. (5.3)	on	off	$\hat{D}(\beta) \otimes \hat{D}(\beta)$	Eq. (5.13)	Eq. (5.14)
ímpar	0	par	0	Eq. (5.3)	on	off	$\hat{D}(\beta) \otimes I$	Eq.(5.16)	Eq. (5.17)
ímpar	0	ímpar	0	Eq. (5.3)	on	off	$I \otimes \hat{D}(\beta)$	Eq. (5.9)	Eq. (5.10)
0	par	par	0	Eq. (5.4)	off	on	$I \otimes I$	1	Eq. (5.6)
0	par	ímpar	0	Eq. (5.4)	off	on	$\hat{D}(\beta) \otimes \hat{D}(\beta)$	Eq. (5.13)	Eq. (5.14)
0	ímpar	par	0	Eq. (5.4)	off	on	$\hat{D}(\beta) \otimes I$	Eq.(5.16)	Eq. (5.17)
0	ímpar	ímpar	0	Eq. (5.4)	off	on	$I \otimes \hat{D}(\beta)$	Eq. (5.9)	Eq. (5.10)
par	0	0	par	Eq. (5.5)	on	on	$I \otimes I$	1	Eq. (5.6)
par	0	0	ímpar	Eq. (5.5)	on	on	$\hat{D}(\beta) \otimes \hat{D}(\beta)$	Eq. (5.13)	Eq. (5.14)
ímpar	0	0	par	Eq. (5.5)	on	on	$\hat{D}(\beta) \otimes I$	Eq.(5.16)	Eq. (5.17)
ímpar	0	0	ímpar	Eq. (5.5)	on	on	$I \otimes \hat{D}(\beta)$	Eq. (5.9)	Eq. (5.10)

Legenda: on/off – ligado e desligado.

Os gráficos a seguir (FIGURAS 5.3, 5.4 e 5.5) mostram as curvas da probabilidade total de sucesso e fidelidade total em função de $|\alpha|^2$, θ e ϕ, sendo $a = \sin(\theta)$, $b = \cos(\theta)$, $c = \sin(\phi)$, $d = \cos(\phi)$ e α são reais. Pode-se observar na FIGURA 5.3, que existe uma relação monotônica entre a probabilidade total de sucesso e a fidelidade total, determinado em (5.18) e (5.19), e o número médio de fótons $|\alpha|^2$, para um circuito óptico sem perda e com contadores de número de fótons ideais, para vários valores de θ e ϕ. Ambos p_T e F_T assintoticamente se aproximam de 1 no limite em que $|\alpha|^2 \to \infty$.

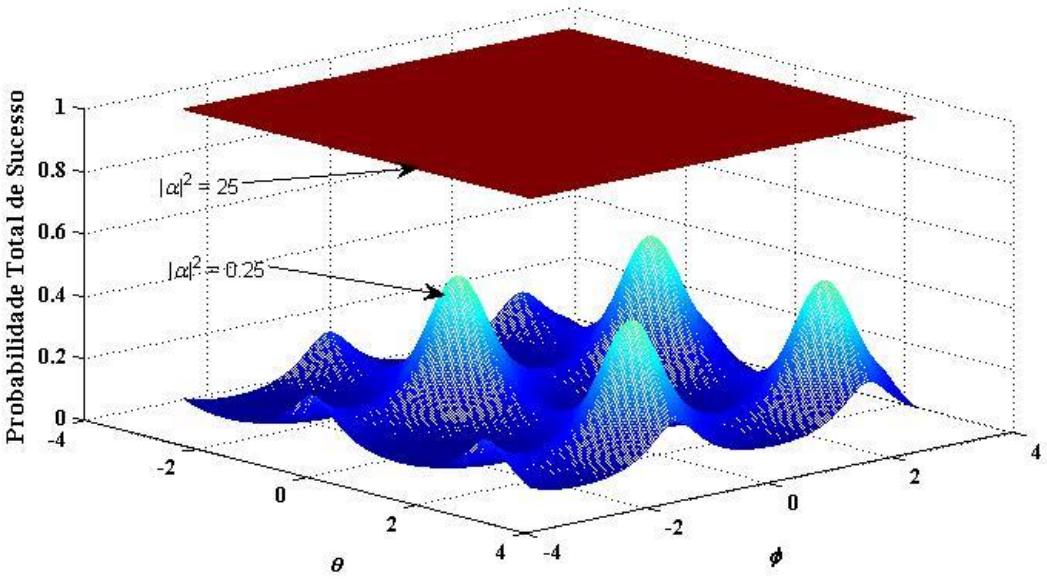
Figura 5.3 – Probabilidade total de sucesso e da fidelidade total versus $|\alpha|^2$ para um sistema óptico sem perdas e contador de número de fótons ideais. (a) $\theta = \pi/4$ e $\phi = \pi/4$; (b) $\theta = \pi/4$ e $\phi = 2\pi/3$; (c) $\theta = \pi/3$ e $\phi = 2\pi/3$.



Fonte: Elaborada pela autora.

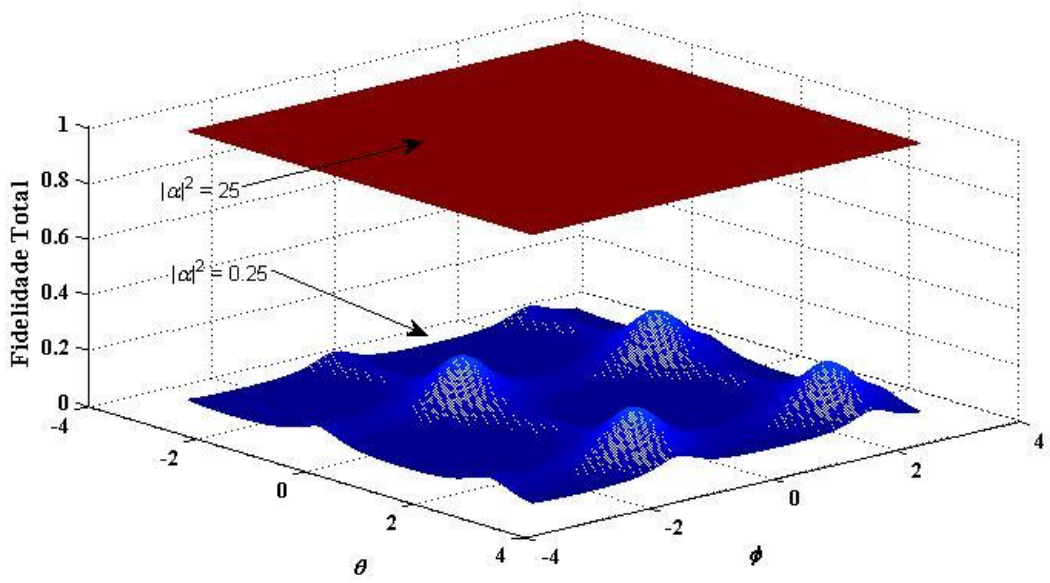
Os gráficos (FIGURAS 5.4 e 5.5) mostram que a porta CNOT proposta é *near-faithful* quando $|\alpha|^2 \geq 25$ e independente de θ e ϕ, isto é, independente dos estados de entrada, $|C\rangle$ and $|T\rangle$.

Figura 5.4 – Probabilidade total de sucesso em função de θ e ϕ para $|\alpha|^2 = 0.25$ e $|\alpha|^2 = 25$.



Fonte: Elaborada pela autora.

Figura 5.5. Fidelidade total em função de θ e ϕ para $|\alpha|^2 = 0.25$ e $|\alpha|^2 = 25$.



Fonte: Elaborada pela autora.

6 CONCLUSÕES E PERSPECTIVAS FUTURAS

As conclusões da presente dissertação são descritas a seguir.

Inicialmente, foram analisados os impactos dos efeitos de PMD e PDL no desempenho de um sistema DQC em redes de comunicação baseado em fibra óptica. Foi descrito um modelo matemático analítico da fidelidade média de um sistema óptico em função dos parâmetros do PMD e PDL e, posteriormente, observou-se como seus efeitos afetam o desempenho de sistemas DQC para o protocolo BB84, quanto a QBER e a taxa de geração de chave segura. Como já observado em sistema de comunicação óptica clássica, os efeitos de PMD e PDL também degradam o desempenho de sistemas QKD. Verificou-se que a taxa de geração de chave, no sistema analisado, decresce à medida que o DGD e PDL aumentam. Portanto, em sistema de comunicação de longa distância, esses efeitos não podem ser negligenciados, portanto, uma compreensão mais detalhada dos mesmos propiciará o desenvolvimento de sistemas DQC mais eficientes e de alcances maiores.

No campo de processamento quântico da informação para qubits codificados em estados coerentes, foram apresentadas duas propostas de circuitos ópticos factíveis de implementação com dispositivos ópticos lineares. O primeiro circuito é um gerador probabilístico de um tipo de estado entrelaçado de quatro modos. Como esperado, a eficiência do gerador melhora com o aumento do número médio de fótons $|\alpha|^2$, apresentando uma eficiência máxima de 25%. O valor de $|\alpha|^2$ tem de ser tão grande quanto possível, a fim de assegurar a ortogonalidade dos estados da base e diminuir a probabilidade de erro nos sistemas de detecções homódinas (o detector pode não disparar devido à baixa eficiência do mesmo e/ou uma grande amplitude grande da componente de vácuo), o que levaria o usuário do sistema a conclusões erradas sobre o estado gerado. O segundo circuito óptico proposto é capaz de implementar probabilisticamente a porta CNOT. Para isso, usa-se uma versão modificada do estado entrelaçado de quatro modos como recurso auxiliar. Um operador de deslocamento apropriado pode ser usado quando o circuito da CNOT falha, de um modo que possa funcionar com alta fidelidade, quando $|\alpha|^2 \geq 25$, independentemente dos estados de entrada. A eficiência total da CNOT óptica é de 25%, considerando a geração do estado entrelaçado de modo quatro.

As perspectivas de trabalhos futuros tendo como base a presente dissertação são descritas a seguir:

- Análise do impacto dos efeitos do PMD e PDL no desempenho em outros sistemas de DQC e proposição de sistemas dinâmicos de compensação desses efeitos.
- Geração de estados entrelaçados de três e quatro modos a partir o gerador óptico proposto para diferentes estados de entradas (estados cat par e ímpar).

REFERÊNCIAS

[1] EINSTEIN, A.; POLDOSKY, B.; ROSEN, N. **"Can quantum mechanical description of physical reality be considered complete?"**. *Phys. Rev. 47, 777–780,* 25 March 1935.

[2] SILVA, J. B. R. **"Sistemas Ópticos para Comunicação e Computação Quânticas"**. *Tese, Universidade Federal do Ceará – UFC*, Fortaleza, 2008.

[3] KNILL, E.; LAFLAMME, R.; MILBURN, G. J. **"A scheme for efficient quantum computation with linear optics"**. *Nature, 409, 46,* 2001.

[4] PITTMAN, T. B.; JACOBS, B. C.; FRANSON, J. D. **"Experimental demonstration of a quantum circuit using linear optics gates"**. *Phys. Rev. A, 71, 032307,* 2005.

[5] SPEDALIERI, F. M.; LEE, H.; DOWLING, J. P. **"High-fidelity linear optical quantum computing with polarization encoding"**. *Phys. Rev. A, 73, 012334,* 2006.

[6] RALPH, T. C.; WHITE, A. G.; MUNRO, W. J.; Milburn, G. J. **"Simple scheme for efficient linear optics quantum gates"**. *Phys. Rev. A, 65, 012314,* 2001.

[7] KOK, P.; MUNRO, W. J.; NEMOTO, K.; RALPH, T. C.; DOWNLING, J. P.; MILBURN, G. J. **"Linear optical quantum computing"**. *Quant-ph/0512071,* 2005.

[8] IMAMOGLU, A. **"Are quantum dots useful for quantum computation?"**. *Phys. E, 16, 47-50,* 2003.

[9] YOU, J. Q.; TSAI, J. S.; NORI, F. **"Experimentally realizable scalable quantum computing using superconducting qubits"**. *Phys. E, 18, 35,* 2003.

[10] MAKHLIN, Y.; SCHÖN, G.; SHNIRMAN, A. **"Josephson junction quantum logic gates"**. *Comp. Phys. Comm., 127, 156,* 2000.

[11] COPSEY, D.; OSKIN, M.; IMPENS, F.; METODIEV, T.; CROSS, A.; CHONG, F. T.; CHUANG, I. L.; KUBIATOWICZ, J. **"Toward a scalable, silicon-based quantum computing architecture"**. *IEEE Journal of Selected Topics in Quantum Electronics, 9, 6, 1552,* 2003.

[12] KAWABATA, S. **"Quantum Information Processing and Entanglement in Solid State Devices"**. *Science and Technology of Advanced Materials 5, 295–299,* 2004.

[13] CHUANG, I. L.; GERSHENFELD, N.; KUBINEC, M. G.; LEUNG, D. W. **"Bulk quantum computation with nuclear magnetic resonance: theory and experiment"**. *Proc. R. Soc. Lond. A., 454, 447,* 1998.

[14] CHUANG, I. L.; VANDERSYPEN, M. K.; ZHOU, X.; LEUNG, D. W; Lloyd, S. **"Experimental realization of a quantum algorithm"**. *Nature, 393, 143,* 1998.

[15] HAVEL, T. F.; SOMAROO, S. S.; TSENG, C.; CORY, D. G. **"Principles and Demonstrations of Quantum Information Processing by NMR Spectroscopy"**. *Appl. Algebra in Eng., Comm. and Comp., 10, 339,* 2000.

[16] CIRAC, J. I.; ZOLLER, P. **"Quantum computations with cold trapped ions"**. *Phys. Rev. Lett., 74: 4091,* 1995.

[17] MONROE, C.; MEEKHOF, D. M.; KING, B. E.; JEFFERTS, S. R; ITANO, W. M.; WINELAND, D. J.; GOULD, P. **"Demonstration of a fundamental quantum logic gate"**. *Phys. Rev. Lett.* **75**, 4714–4717, 1995.

[18] BRAUNSTEIN, S. L.; KIMBLE, H. J. **"Teleportation of Continuous Quantum Variables"**. *Phys. Rev. Lett., 80, 869,* 1998.

[19] VASCONCELOS, H. H. M. **"Topics in coherent state quantum computation and state purification"**. *Thesis, Graduate Program in Physics Notre Dame,* Indiana, 2006.

[20] RALPH, T. C.; GILCHRIST, A.; MILBURN, G. J.; GLANCY, S. **"Quantum computation with optical coherent states"**. *Phys. Rev. A, 68, 042319,* 2003.

[21] JEONG, H.; KIM, M. **"Efficient quantum computation using coherent states"**. *Phys. Rev. A, 65, 042305,* 2002.

[22] PLANTENBERG, J. H; GROOT, P. C.; HARMANS, C. J. P. M.; MOOIJ , J. E. **"Demonstration of controlled-NOT quantum gates on a pair of superconducting quantum bits"**. *Nature 447, 836-839,* 2007.

[23] GLANCY, S.; VASCONCELOS, H. H. M.; RALPH, T. C., **"Transmission of optical coherent state qubits"**. *Phys. Rev. A, 70, 22317,* 2004.

[24] O'BRIEN, J. L.; PRYDE, G. J.; WHITE, A. G.; RALPH, T. C; BRANNING, D. **"Demonstration of an all-optical quantum controlled-NOT gate"**. *Nature, 426, 264-267,* 2003.

[25] PITTMAN, T. B.; JACOBS, B. C.; FRANSON, J. D. **"Probabilistic quantum encoder for single-photon qubits"**. *Phys. Rev. A, 69, 042306,* 2004.

[26] PITTMAN, T. B.; JACOBS, B. C.; FRANSON, J. D. **"Demonstration of feed-forward control for linear optics quantum computation"**. *Phys. Rev. A, 66, 052305,* 2002.

[27] RALPH, T. C.; LANGFORD, N. K.; BELL, T. B; WHITE, A. G. **"Linear optical controlled-NOT gate in the coincidence basis"**. *Phys. Rev. A, 65, 062324,* 2002.

[28] HOFMANN, H. F.; TAKEUCHI, S. **"Quantum phase gate for photonic qubits using only beam splitters and postselection"**. *Phys. Rev. A, 66, 024308,* 2002.

[29] PITTMAN, T. B.; FITCH, M. J.; JACOBS, B. C.; FRANSON, J. D. **"Experimental controlled-NOT logic gate for single photons in the coincidence basis"**. *Phys. Rev. A, 68, 032316,* 2003.

[30] HUANG, Y. F.; REN, X. F.; ZHANG, Y. S.; DUAN, L.M.; GUO, G. C. **"Experimental Teleportation of a Quantum Controlled-NOT Gate"**. *Phys. Rev. Lett., 93, 240501,* 2004.

[31] FIORENTINO, M.; KIM, T.; WONG, F. N. C. **"Single-photon two-qubit SWAP gate for entanglement manipulation"**. *Phys. Rev. A, 72, 012318,* 2005.

[32] ZOU, X. B.; LI, K.; GUO, G. C. **"Linear optical scheme for direct implementation of a nondestructive N-qubit controlled phase gate"**. *Phys. Rev. A, 74, 044305,* 2006.

[33] ZOU, X. B.; ZHANG, S. L.; LI, K.; GUO, G. C. **"Linear optical implementation of the two-qubit controlled phase gate with conventional photon detectors"**. *Phys. Rev. A, 75, 034302,* 2007.

[34] ČERNOCH, A.; SOUBUSTA, J.; BARTŮŠKOVÁ, L.; DUŠEK, M.; FIURÁŠEK, J. **"Experimental Realization of Linear-Optical Partial swap Gates"**. *Phys. Rev. Lett., 100, 180501,* 2008.

[35] FIURÁŠEK, J. **"Linear optical Fredkin gate based on partial-SWAP gate"**. *Phys. Rev. A, 78, 032317,* 2008.

[36] HONG-FU, W.; SHOU, Z. **"Application of quantum algorithms to direct measurement of concurrence of a two-qubit pure state"**. *Phys. B, 18, 2642,* 2009.

[37] SHI-QING, T.; DENG-YU, Z.; XIN-WEN, W.; LI-JUN, X.; FENG, G. **"Feasible schemes for quantum swap gates of optical qubits via cavity QED"**. *Phys. B, 20, 040308,* 2011.

[38] HONG-FU, W.; SHOU, Z.; AI-DONG, Z. **"Deterministic implementations of fermionic quantum SWAP and Fredkin gates for spin qubits based on charge detection"**. *Phys. B, 21, 040306,* 2012.

[39] NIELSEN, M. A.; CHUANG, I. L. **"Quantum Computation and Quantum Information".** *Reprinted, Cambridge University Press,* 2003.

[40] SILVA, J. B. R.; RAMOS, R. V. **"Implementations of quantum and classical gates with linear optical devices and photon number quantum non-demolition measurement for polarization encoded qubits"**. *Phys. Lett. A, 359, 592,* 2006.

[41] NEMOTO, K.; MUNRO, W. J. **"Nearly Deterministic Linear Optical Controlled-NOT Gate"**. *Phys. Rev. Lett., 93, 250502,* 2004.

[42] FERNANDEZ, V.; COLLINS, R. J.; GORDON, K. J. Gordon; BULLER, G. S**. "Passive Optical Network Approach to GigaHertz - Clocked Multiuser Quantum Key Distribution"**. *School of Engineering and Physical Sciences, Heriot-Watt University, Edinburgh, EH14 AS, UK. IEEE Journ,* p. 130–138, 2007.

[43] SCARANI, V. **"Classical and quantum: some mutual"**. *Group of Applied Physics, University of Geneva,* Switzerland, 2002.

[44] SCARANI, V.; HELLE, B. P.; CERF, N. J.; DUSEK, M.; LUTKENHAUS, **N.; Peev, M**. **"The Security of Practical Quantum Key Distribution"**. *Centre for Quantum Technologies and Department of Physics, National University,* 2009.

[45] JEONG, Y.-C.; KIM, Y.-S.; KIM, Y.-H. **"Effects of depolarizing quantum channels on BB84 and SARG04 quantum cryptography protocols"**. *Department of Physics, Pohang University of Science and Technology (POSTECH), Pohang, 790-784, Korea,* 2011.

[46] DAMASK, Jay N. **"*Polarization Optics in Telecommunications*".** SPRINGER pp.297-384, 2004.

[47] AGRAWAL, G. P. **"Lightwave Technology: Telecomunication Systems"**. *Ed. A John Wiley & Sons, Hoboken, New Jersey,* pp. 63–101, 1951.

[48] OLIVEIRA, M. S. R.; SILVA, J. B. R. **"Análise do Impacto do PMD e PDL no Desempenho de um Sistema de Distribuição Quântica de Chaves Baseado no Protocolo BB84"**. *III Workshop-Escola de Computação e Informação Quântica,* Petrópolis, Rio de Janeiro, 2010.

[49] KRAUS, B.; BRANCIARD, C.; RENNER, R. **"Security of quantum-key-distribution protocols using two-way classical communication or weak coherent pulses"**. *Phys. Rev. A 75, 012316,* 2007.

[50] LJUNGGREN, D. **"Entanglement in quantum communication – preparation and caracterization of photonics qubits"**. *Thesis, KTH School of Information and Communication Technology, Stockhlm, Sweden,* 2006.

[51] GLAUBER, R. J. **"The quantum theory of optical coherence"**. *Phys. Rev., 130, 2529,* 1963.

[52] LUND, A. P.; RALPH, T. C.; HASELGROVE, H. L. **"Fault-tolerant linear optical quantum computing with small-amplitude coherent states"**. *Phys. Rev. Lett. 100, 030503* 2008.

[53] STOBINSKA, M.; MILBURN, G. J.; WODKIEWICZ, K. **"Effective generation of cat and kitten states"**. *Presented at the 38th Symposium on Mathematical Physics "Quantum Entanglement & Geometry*", 2006. *arXiv:quant-ph/0610256v1,* 30 Oct 2006.

[54] KRAUS, B.; CIRAC, J. I. **"Optimal creation of entanglement using a two-qubit gate"**. *Phys. Rev. A, 63, 062309,* 2001.

[55] SILVA, J. B. R.; RAMOS, R. V. **"Smart generation of a tripartite GHZ-type state for coherent state qubit"**. *Optics Communications, Volume 281, Issue 9, pp. 2705–2709,* 2008.

[56] GISIN, N.; RIBORDY, G.; TITTEL, W.; Zbinden, H. **"Quantum cryptography"**. *Rev. Mod. Phys. 74, 145,* 2002.

[57] ZHOU, G.; XU, K.; WU, J.; LIN, J. **"Analysis of DOP feedback signal in PMD compensation system based on the different modulation formats"**. *Proc. SPIE 5625, Optical Transmission, Switching, and Subsystems II, 628; doi:10.1117/12.575435,* 2005.

[58] DIAMANTI, E. **"Security and Implementation of Differentiall Phase Shift Quantum Key Distribution Systems"**. *Stanford University*, Master Thesis, 2006.

[59] FUNG, C.-H. F., **"Security and Performance Analyses of Quantum-Key-Distribution Systems"**. *Thesis, University of Toronto,* 2008.

[60] BRUNNER, N.; ACÍN, A.; COLLINS, D.; GISIN, N.; SCARANI, V. **"Optical Telecom Networks as Weak Quantum Measurements with Postselection"**. *Phys. Rev. Lett. 91, 180402,* 2003.

[61] HUTTNER, B.; GEISER, C.; GISIN, N. **"Polarization-induced distortions in optical fiber networks with polarization-mode dispersion and polarization-dependent losses"**. *IEEE J. Sel. Top. Quant. Electron. vol.6, no.2, p. 317-329,* 2000.

[62] AGRAWAL, G. P. **"Lightwave Technology: Telecomunication Systems"**. *Ed. A John Wiley & Sons, Hoboken, New Jersey,* pp.63–103, 2005.

[63] JEONG, Y.-C.; KIM, Y.-S.; KIM, Y.-H. **"Effects of depolarizing quantum channels on BB84 and SARG04 quantum"**. *PACS numbers: 03.67.Dd, 03.67.Hk, 42.79.Sz, 1002.2285v1,* 2010.

[64] ZHANG, S. L.; ZOU, X.; JIN, C.-H.; GUO, G. C. **"Closing the gap of secure quantum key rate with the Heralded Pair-Coherent States"**. *Quant-ph, arXiv:0807.1760v1,* 2008.

[65] CHEN, L.; ZHANG, Z.; BAO, X. **"Combined PMD-PDL effects on BERs in simplified optical systems: an analytical approach"**. *Optics Express, Department of Physics, University of Ottawa, Ottawa,* Vol. 15, No. 5, 2007.

[66] FERREIRA, M. F. **"Evaluation of higher order PMD effects using Jones matrix analytical models: a comparative study"**. *Proc. SPIE,* Vol. 6193, pp. 619308-1–619308-9, 2006.

[67] ZHANG, Y.; YANG, C.; LI, S. **"Impact of polarization dependent loss on degree of polarization as feedback signal of polarization mode dispersion"**. *Chinese Optics Letters,* Vol. 4, Issue 1, pp.1-3, 2006.

[68] NEZAM, M.; REZA, S. M.; McGEEHAN, J. E.; et al. **"Theoretical and Experimental Analysis of the Dependence of a Signal's Degree of Polarization on the Optical Data Spectrum"**. *Journal of Lightwave Technology,* Vol. 22, Issue 3, p.763, 2004.

[69] XIE,C.; MOLLENAUER, L. F. **"Performance Degradation Induced by Polarization Dependent Loss in Optical Fiber Transmission Systems With and Without Polarization Mode Dispersion"**. *IEEE Journal of Lightwave Technology,* Vol. 21, 9, pp. 1953 – 1957, 2003.

[70] REZA, S. M.; McGEEHAN, J. E. **"Theoretical and Experimental Analysis of the Dependence of a Signal's Degree of Polarization on the Optical Data Spectrum"**. *IEEE Journal of Lightwave Technology,* Vol. 22, no. 3, 2004.

[71] GOTTESMAN, D.; LO, H.-K.; LÜTKENHAUS, N.; Preskill, J. **"Security of quantumkey distribution with imperfect devices"**. *Quantum Information and Computation,* Vol. 5, pp. 325–360, 2004.

[72] LO, H.-K. **"Getting something out of nothing"**. *Quantum Inf. Comput.,* 5, 413, 2005.

[73] PITTMAN, T. B.; JACOBS, B. C.; FRANSON, J. D. **"Probabilistic quantum logic operations using polarizing beam splitters"**. *Phys. Rev. A, 64, 062311,* 2001.

[74] PHOENIX, S. J. D.; TOWNSEND, P. D. **"Quantum cryptography: how to beat the code breaks using quantum mechanics"**. *Contemporary Phys., 36, 165-195,* 1995.

[75] BARTLETT, S. D.; GUISE, H. ; SANDERS, C. **"Quantum encodings in spin systems and harmonic oscillators"**. *Phys. Rev. A, 65, 052316,* 2002.

[76] JEONG, H. J.; KIM, M. S.; RALPH, T. C.; HAM, B. S. **"Generation of macroscopic superposition states with small nonlinearity"**. *Phys. Rev. A, 70, 061801(R),* 2004.

[77] LUND, A. P.; JEONG, H.; RALPH, T. C.; KIM, M. S. **"Conditional production of superpositions of coherent states with inecient photon"**. *Phys. Rev. A, 70, 20101,* 2004.

[78] JEONG, H.; LUND, A. P.; RALPH, T. C. **"Production of superpositions of coherent states in traveling optical fields with inefficient photon detection"**. *Phys. Rev A, 72, 13801,* 2005.

[79] OURJOUMTSEV, A.; TUALLE-Brouri, R.; LAURAT, J.; GRANGIER, P. **"Generating optical Schrödinger kittens for quantum information processing"**. *Science, 312, 83-86,* 2006.

[80] GLANCY, S.; VASCONCELOS, H. H. M. **"Methods for producing optical coherent state superpositions"**. *J. Opt. Soc. Am. B, 25, 712-733,* 2008.

[81] YE, M.-Y.; LIN, X.-M. **"A genuine four-partite entangled state"**. *Physics Letters A 372, 4157–4159,* 2008.

[82] JEONG, H.; AN, N. B. **"Greenberger-Horne-Zeilinger–type and W-type entangled coherent states: Generation and Bell-type inequality tests without photon counting"**. *Phys. Rev. A, 74, 022104,* 2006.

[83] GLÖCKL, O.; LORENZ, S.; MARQUARDT, C., et al. **"Experiment towards continuous-variable entanglement swapping: Highly correlated four-partite quantum state"**. *Phys. Rev. A, 68, 01231–9,* 2003.

[84] GONTA, D.; FRITZSCHE, S.; RADTKE, T. **"Generation of four-partite Greenberger-Horne-Zeilinger and W states by using a high-finesse bimodal cavity"**. *Phys. Rev. A, 77, 062312,* 2008.

[85] WANG, Y.; SU, X.; SHEN, H.; et al. **"Toward demonstrating controlled-X operation based on continuous-variable four-partite cluster states and quantum teleporters"**. *Phys. Rev. A, 81, 022311,* 2010.

[86] TAN, A.; WANG, Y.; JIN, X.; et al. **"Experimental generation of genuine four-partite entangled states with total three-party correlation for continuous variables"**. *Phys. Rev. A 78, 01382,* 2008.

[87] PRAKASH, H.; CHANDRA, N.; PRAKASH, R.; et al. **"Almost Perfect Teleportation Using 4-Partite Entangled states"**. *International Journal of Modern Physics B, Vol. 24, No. 17, 3383–3394,* 2010.

[88] NA-Hui, C.; JIN-Ming, L. **"Teleportation of a Bipartite Entangled Coherent State via a Four-Partite Cluster-Type Entangled State"**. *Commun. Theor. Phys. (Beijing, China) 52,* Vol. 52, No. 4, pp. 597–600, 2009.

[89] SOUSA, P. B. M.; SILVA, J. B. R.; RAMOS, R. V. **"Implementing non-local xor function with quantum communication"**. *J. of Mod. Opt., 53, 1765,* 2006.

[90] OLIVEIRA, M. S. R.; VASCONCELOS, H. H. M.; SILVA, J. B. R. **"A New Proposal of a Probabilistic CNOT Gate for Coherent-State Qubits"**. *IV Workshop-School on Quantum Computation and Information (WECIQ-2012),* p. 160, 2012.

[91] OLIVEIRA, M. S. R.; VASCONCELOS, H. H. M.; SILVA, J. B. R. **"Generation of a Four-Mode-Type Entangled State for Coherent-States Qubit"**. *IV Workshop-School on Quantum Computation and Information (WECIQ-2012),* pp. 120-123, 2012.

APÊNDICE A – CÁLCULO DA FIDELIDADE MÉDIA EM FUNÇÃO DOS PARÂMETROS PMD E PDL

Neste Apêndice, apresentar-se-ão os passos importantes para entendimento do cálculo da expressão analítica da fidelidade média em função dos parâmetros do PMD e do PDL presentes em enlace de fibra óptica.

Inicialmente, deve-se considerar os valores das funções de autocorrelação e de densidade espectral, que deverão ser usadas no decorrer do desenvolvimento teórico, como sendo, respectivamente:

$$R(\tau) = \frac{1}{2\pi}\int_{-\infty}^{+\infty} S(\omega) e^{j\omega\tau} d\omega; \tag{A.1}$$

$$S(\omega) = \lim_{\tau\to\infty} \frac{\left|A(\omega)\right|^2}{\tau}. \tag{A.2}$$

Sendo, o estado de entrada $|\Psi_{in}\rangle$, no domínio do tempo, um pulso de luz Gaussiano de tempo de coerência τ_c (g(t)) e de frequência central ω_0, preparado em um estado de polarização puro $|\psi_0\rangle = (\varepsilon|H\rangle + \lambda|V\rangle)$ [60], é apresentado como:

$$\left|\Psi_{in}\right\rangle = g(t) \otimes \left(\varepsilon\left|H\right\rangle + \lambda\left|V\right\rangle\right) \Leftrightarrow \left|\Psi_{in}\right\rangle_{\omega} = G(\omega)\left(\varepsilon\left|H\right\rangle + \lambda\left|V\right\rangle\right), \tag{A.3}$$

onde $\mathrm{g}(t) = \mathcal{A}\, e^{-t^2/4t^2_c}$ e a transformada de Fourier de g(t) correspondente :

$G(\omega) = \int_{-\infty}^{+\infty} \mathrm{g}(t) e^{-j\omega t}$.

Assim, ter-se-á o seguinte estado na saída $|\Psi_{out}\rangle_{\omega} = \mathrm{U_{PDL}}\ \mathrm{U_{PMD}}\ |\Psi_{in}\rangle_{\omega}$ e $N = [(|\varepsilon|^2 e^{\alpha} + |\lambda|^2 e^{-\alpha})]^{-1/2}$, resultando conforme abaixo:

$$\left|\Psi_{out}\right\rangle_{\omega} = NG(\omega)\left(\varepsilon e^{\alpha/2} e^{j\omega b/2}\left|H\right\rangle + \lambda e^{-\alpha/2} e^{-j\omega b/2}\left|V\right\rangle\right). \tag{A.4}$$

Seja $g(t)$ um processo estocástico, a fidelidade média $\mathcal{F}$ considerando o operador $\mathrm{U_{PMD}}$ (3.1) e $\mathrm{U_{PDL}}$ (3.2), é:

$$\mathcal{F} = \lim_{\tau\to\infty} \frac{1}{2\pi t_c}\int_{-\infty}^{+\infty} E\left\{\left|\left\langle \Psi_{in} \middle| \Psi_{out}\right\rangle_{\omega}\right|\right\} d\omega. \tag{A.5}$$

Tomando a expressão de $\langle \Psi_{in} | \Psi_{out} \rangle_{\omega}$, como:

$$\begin{aligned}\left\langle \Psi_{in} \middle| \Psi_{out} \right\rangle_{\omega} &= \left\langle \Psi_{in} \middle| U_{PDL} U_{PMD} \middle| \Psi_{in} \right\rangle \\ &= G^{*}(\omega)\left(\varepsilon^{*} \left\langle H \right| + \lambda^{*} \left\langle V \right|\right) NG(\omega)\left(\varepsilon e^{\alpha/2} e^{j\omega b/2} \left| H \right\rangle + \lambda e^{-\alpha/2} e^{-j\omega b/2} \left| V \right\rangle\right) \\ &= N\left|G(\omega)\right|^{2}\left(\left|\varepsilon\right|^{2} e^{\alpha/2} e^{j\omega b/2} + \left|\lambda\right|^{2} e^{-\alpha/2} e^{-j\omega b/2}\right).\end{aligned} \tag{A.6}$$

Agora, substituindo (A.6) em (A.5), tem-se:

$$\begin{aligned}\mathcal{F} &= \lim_{\tau\to\infty} \frac{1}{2\pi t_c} \int_{-\infty}^{+\infty} N\left(\left|\varepsilon\right|^{2} e^{\alpha/2} e^{j\omega b/2} + \left|\lambda\right|^{2} e^{-\alpha/2} e^{-j\omega b/2}\right) E\left\{\left|G(\omega)\right|^{2}\right\} d\omega \\ &= \frac{1}{2\pi} N\left\{\left|\varepsilon\right|^{2} e^{\alpha/2} \lim_{t_c\to\infty} \int_{-\infty}^{+\infty} \frac{E\left\{\left|G(\omega)\right|^{2}\right\} e^{j\omega b/2} d\omega}{t_c} + \left|\lambda\right|^{2} e^{-\alpha/2} \lim_{t_c\to\infty} \int_{-\infty}^{+\infty} \frac{E\left\{\left|G(\omega)\right|^{2}\right\} e^{-j\omega b/2} d\omega}{t_c}\right\},\end{aligned} \tag{A.7}$$

sendo $S(\omega) = \lim_{t_c\to\infty} \dfrac{E\left\{\left|G(\omega)\right|^{2}\right\}}{t_c}$.

Então,

$$\mathcal{F} = N\left\{\left|\varepsilon\right|^{2} e^{\alpha/2} \frac{1}{2\pi} \int_{-\infty}^{+\infty} S(\omega) e^{j\omega b/2} d\omega + \left|\lambda\right|^{2} e^{-\alpha/2} \frac{1}{2\pi} \int_{-\infty}^{+\infty} S(\omega) e^{-j\omega b/2} d\omega\right\}, \tag{A.8}$$

mas, substituindo a equação $R(\tau) = \dfrac{1}{2\pi} \displaystyle\int_{-\infty}^{+\infty} S(\omega) e^{j\omega b/2} d\omega,$ que é a função de autocorrelação de $g(t)e^{j\omega t}$, onde faz-se $\tau = b$, finalmente, chega-se à expressão da fidelidade média:

$$\mathcal{F} = N\left\{\left|\varepsilon\right|^{2} e^{\alpha/2} R(b/2) + \left|\lambda\right|^{2} e^{-\alpha/2} R(-b/2)\right\}. \tag{A.9}$$

Considerar os seguintes valores para α: $-0{,}1 \le \alpha \le 0{,}1$.

APÊNDICE B - CÁLCULO DA PROBABILIDADE DE SUCESSO DO GERADOR

Este Apêndice demonstra à análise da probabilidade de sucesso do Gerador de um tipo de estado entrelaçado de quatro modos para qubit de estado coerente, proposto no Capítulo 4.

Tem-se que a probabilidade de sucesso do gerador é dada como segue:

$$P_{succ} = P_{\rho 1} + P_{\rho 2} + P_{\rho 3} + P_{\rho 4}. \tag{B.1}$$

E considerando que para detectores ideais, deve-se ter:

$$P_{\rho 1} = P_{1001} \left\langle \Psi_{\det} \middle| \rho_1 \middle| \Psi_{\det} \right\rangle. \tag{B.2}$$

Assim, a probabilidade de sucesso do gerador é dada pela probabilidade condicional, sendo P_n a probabilidade de ocorrer um clique no detector n, desde que o estado de entrada seja diferente do estado vácuo ($|0\rangle$), logo: $P_n = 1 - P_{\langle 0|\pm\infty\rangle}$, onde $P_{\langle 0|\pm\infty\rangle}$ é a probabilidade de medição de zero fóton para o estado $|\pm\infty\rangle$.

Ou seja, $P_{\langle 0|\pm\infty\rangle} = \left|\langle 0|\pm\infty\rangle\right|^2 = e^{-|\alpha|^2}$.

Assim, $P_n = 1 - e^{-|\alpha|^2}$.

E a probabilidade de detectar o estado vácuo é $P_0 = 1$, uma vez que os detectores são ideais, ou seja: $P_2 = P_3 = 1$ e $P_1 = P_4 = 1 - e^{-|\alpha|^2}$.

Logo, $P_{1001} = P_1 P_2 P_3 P_4 = \left(1 - e^{-|\alpha|^2}\right)^2$.

$$\left\langle \Psi_{\det} \middle| \rho_1 \middle| \Psi_{\det} \right\rangle = \left\langle \Psi_{\det} \middle| \rho_1 \right\rangle \left\langle \rho_1 \middle| \Psi_{\det} \right\rangle = \left| \left\langle \Psi_{\det} \middle| \rho_1 \right\rangle \right|^2. \tag{B.3}$$

$$\begin{aligned} \left\langle \Psi_{\det} \middle| \rho_1 \right\rangle &= N_{\varepsilon}^{\otimes 6} \left\{ \frac{1}{N^*} \left(\left\langle \Psi_1 \right| + \left\langle \Psi_2 \right| + \left\langle \Psi_3 \right| + \left\langle \Psi_4 \right| \right) + \frac{\left\langle \Psi_u \right|}{N_u} \right\} \middle| \Psi_1 \right\rangle \\ &= N_{\varepsilon}^{\otimes 6} \left\{ \frac{1}{N^*} \left(1 + \left\langle \Psi_2 \middle| \Psi_1 \right\rangle + \left\langle \Psi_3 \middle| \Psi_1 \right\rangle + \left\langle \Psi_4 \middle| \Psi_1 \right\rangle \right) + \frac{\left\langle \Psi_u \middle| \Psi_1 \right\rangle}{N_u} \right\}. \end{aligned} \tag{B.4}$$

Assim,

$$\left|\left\langle \Psi_{\det} \middle| \Psi_1 \right\rangle\right|^2 = \frac{\left|N_\varepsilon\right|^{12}}{4\left|N\right|^2}. \tag{B.5}$$

Portanto,

$$\begin{aligned} P_{\rho 1} &= P_{1001}\left\langle \Psi_{\det} \middle| \rho_1 \middle| \Psi_{\det} \right\rangle = \frac{\left|N_\varepsilon\right|^{12}}{4\left|N\right|^2}\left(1-e^{-|\alpha|^2}\right)^2 \\ &= \frac{\left(1-e^{-|\alpha|^2}\right)^2\left(1+e^{-|\alpha|^2}\right)^6}{16\left(1+e^{-4|\alpha|^2}+2e^{-6|\alpha|^2}\right)}. \end{aligned} \tag{B.6}$$

Mas, $P_{\rho 1} = P_{\rho 2} = P_{\rho 3} = P_{\rho 4}$.

Logo $P_{real} = 4P_{\rho 1}$.

Para detectores reais com eficiência quântica η e probabilidade de contagem de escuro P_{dark}, a probabilidade de haver uma detecção quando o estado de entrada no detector for diferente do estado vácuo será: $P_n = 1-e^{-|\alpha|^2\eta}\left(1-P_{dark}\right)$.

E a probabilidade de detectar o estado vácuo será $P_0 = \left(1-P_{dark}\right)$.

Considerando o caso anterior, a probabilidade de P_{1001} será:

$$P_{1001} = \left(1-P_{dark}\right)^2\left[1-e^{-|\alpha|^2\eta}\left(1-P_{dark}\right)\right]. \tag{B.7}$$

Logo,

$$\begin{aligned} P_{real} &= \left(1-P_{dark}\right)^2\left[1-e^{-|\alpha|^2\eta}\left(1-P_{dark}\right)\right]\frac{\left|N_\varepsilon\right|^2}{\left|N\right|^2} \\ &= \frac{\left(1-P_{dark}\right)^2\left[1-e^{-|\alpha|^2\eta}\left(1-P_{dark}\right)\right]^2\left(1+e^{-2|\alpha|^2}\right)^6}{4\left(1+e^{-4|\alpha|^2}+2e^{-6|\alpha|^2}\right)}. \end{aligned} \tag{B.8}$$

APÊNDICE C - OPERADOR DE DESLOCAMENTO

Este Apêndice apresenta o uso do operador de deslocamento, de forma a melhorar a fidelidade da porta CNOT, mostrados nas expressões (5.8), (5.12) e (5.15) do Capítulo 5.

Considerando que o operador de deslocamento seja dado por:

$$\hat{D}_m(\beta)\left|\varphi\right\rangle_m = e^{j\,\mathrm{Im}(\beta\varphi^*)}\left|\beta+\varphi\right\rangle_m . \tag{C.1}$$

Sendo, $\beta = -\dfrac{j\pi}{4\alpha}$.

Assim, para qubit igual a $|\text{-}\alpha\rangle$, tem-se:

$$\hat{D}\left(\frac{-j\pi}{4\alpha}\right)\left|-\alpha\right\rangle = e^{j\,\mathrm{Im}\left[\frac{-j\pi}{4\alpha}(-\alpha)\right]}\left|\frac{-j\pi}{4\alpha}-\alpha\right\rangle = e^{(+j\pi/4)}\left|\left(\frac{-j\pi}{4\alpha}-\alpha\right)\right\rangle, \tag{C.2}$$

e para qubit igual a $|\alpha\rangle$, tem-se:

$$\hat{D}\left(\frac{-j\pi}{4\alpha}\right)\left|\alpha\right\rangle = e^{j\,\mathrm{Im}\left[\frac{-j\pi}{4\alpha}(\alpha)\right]}\left|\frac{-j\pi}{4\alpha}+\alpha\right\rangle = e^{(-j\pi/4)}\left|\left(\frac{-j\pi}{4\alpha}+\alpha\right)\right\rangle. \tag{C.3}$$

Dessa forma, tome como exemplo o cálculo de $|\phi_1'\rangle$:

$$\left|\phi_1\right\rangle = N_1\left(ac\,|-\alpha,-\alpha\rangle - ad\,|-\alpha,\alpha\rangle - bc\,|\alpha,\alpha\rangle + bd\,|\alpha,-\alpha\rangle\right),$$

onde, $N_1 = \left\{1-2\left[cd\left(1-2ab\right)+abe^{-2|\alpha|^2}\right]e^{-2|\alpha|^2}\right\}^{-1/2}$.

Sendo $e^{\frac{-j\pi}{2}} = \cos\left(-\dfrac{\pi}{2}\right) + j\,sen\left(-\dfrac{\pi}{2}\right) = -j$,

Tem-se, finalmente, a expressão correspondente de $|\phi_1'\rangle$:

$$\begin{aligned}\left|\phi_1'\right\rangle = \hat{D}_2\left(-\frac{j\pi}{4\alpha}\right)\left|\phi_1\right\rangle &= N_1\left(e^{j\pi/4}ac\left|-\alpha,-\frac{j\pi}{4\alpha}-\alpha\right\rangle - e^{j\pi/4}ad\left|-\alpha,-\frac{j\pi}{4\alpha}+\alpha\right\rangle - e^{j\pi/4}bc\left|\alpha,-\frac{j\pi}{4\alpha}+\alpha\right\rangle + e^{j\pi/4}bd\left|\alpha,-\frac{j\pi}{4\alpha}-\alpha\right\rangle\right),\\ &= N_1 e^{j\pi/4}\left(ac\left|-\alpha,-\frac{j\pi}{4\alpha}-\alpha\right\rangle + jad\left|-\alpha,-\frac{j\pi}{4\alpha}+\alpha\right\rangle + jbc\left|\alpha,-\frac{j\pi}{4\alpha}+\alpha\right\rangle + bd\left|\alpha,-\frac{j\pi}{4\alpha}-\alpha\right\rangle\right).\end{aligned}$$