

Universidade Federal do Ceará
Centro de Tecnologia
Departamento de Engenharia de Teleinformática
Programa de Pós-Graduação em Engenharia de Teleinformática

Fábio Alencar Mendonça

**ANÁLISE TEÓRICA E RESULTADOS EXPERIMENTAIS DE
SISTEMAS DE DISTRIBUIÇÃO QUÂNTICA DE CHAVES USANDO
FÓTONS ISOLADOS E ESTADOS COERENTES MESOSCÓPICOS**

**FORTALEZA – CEARÁ
SETEMBRO – 2006**



Universidade Federal do Ceará

Centro de Tecnologia

Departamento de Engenharia de Teleinformática

Programa de Pós-Graduação em Engenharia de Teleinformática

Fábio Alencar Mendonça

**ANÁLISE TEÓRICA E RESULTADOS EXPERIMENTAIS DE
SISTEMAS DE DISTRIBUIÇÃO QUÂNTICA DE CHAVES USANDO
FÓTONS ISOLADOS E ESTADOS COERENTES MESOSCÓPICOS**

Orientador:

Dr. Rubens Viana Ramos

Dissertação submetida à Coordenação do Programa de Pós-Graduação em Engenharia de Teleinformática da Universidade Federal do Ceará, como requisito para obtenção do grau de *Mestre em Engenharia de Teleinformática – Área de Concentração em Eletromagnetismo Aplicado*.

**FORTALEZA – CEARÁ
SETEMBRO – 2006**

M495a Mendonça, Fábio Alencar

Análise teórica e resultados experimentais de sistemas de distribuição quântica de chaves usando fótons isolados e estados coerentes mesoscópicos / Fábio Alencar Mendonça. Orientador: Dr. Rubens Viana Ramos.

117 f.

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

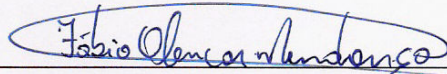
1. Teleinformática. 2. Comunicações óticas. 3. Criptografia de dados. I. Título.

621.38

Fábio Alencar Mendonça

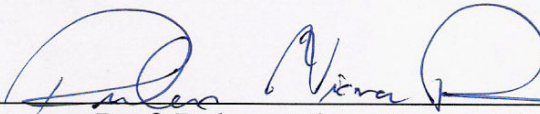
**Análise Teórica e Resultados Experimentais de Sistemas de
Distribuição Quântica de Chaves Usando Fótons Isolados e Estados
Coerentes Mesoscópicos**

Esta dissertação foi julgada adequada para obtenção do título de Mestre em Engenharia de Teleinformática e aprovada em sua forma final pelo Programa de Pós-Graduação em Engenharia de Teleinformática da Universidade Federal do Ceará.

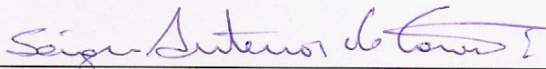


Fábio Alencar Mendonça

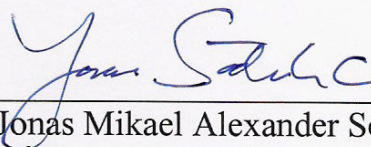
Banca Examinadora:



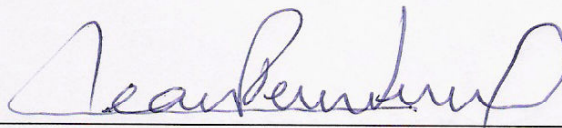
Prof. Rubens Viana Ramos, Dr.



Prof. Sérgio Antenor de Carvalho, Dr.



Prof. Jonas Mikael Alexander Söderholm, Dr.



Prof. Jean Pierre Von der Weid, Dr. ^

Fortaleza, 14 de Setembro de 2006.

*Dedico este trabalho à minha esposa e filho,
Janielle e Carlos Ícaro, aos meus queridos pais
Francisco e Maria Brígida, e meus irmãos
Franciberg, Romário e Bruna. Este trabalho é para
todos vocês.*

Agradecimentos

Ao meu Senhor Deus, que sempre me guia e me ilumina pelos caminhos da vida.

Aos meus amados pais Francisco e Maria Brígida que com amor, humildade e dedicação souberam me educar e sempre acreditaram no meu potencial. Aos meus irmãos Berg, Romário e Bruna. A todos meus demais familiares.

À Janielle, minha querida e amada esposa, que com seu amor, apoio e dedicação contribuiu diretamente na realização deste trabalho. Não poderia esquecer de meu filho Carlos Ícaro que, mesmo nos meus momentos de profundo cansaço, sabia despertar em mim com seus “truques” inocentes a vontade de sempre seguir em frente. À Dona Mara, minha sogra, e meus cunhados Alexandre, Jéssica e Anderson.

Ao amigo, compadre e irmão George Thé, pelo companheirismo e apoio na nossa caminhada desde os tempos do CEFET, Engenharia Elétrica até a Pós-graduação; pelas noites de estudos, instantes de descontração, conselhos e momentos em família.

Ao amigo e Prof. Rubens Viana Ramos, pelos anos de companheirismo e trabalho; pela paciência, confiança e aceitação em orientar e desenvolver esta dissertação e os experimentos do nosso protótipo de distribuição quântica de chaves; por ter sido essencial na minha iniciação à pesquisa.

Aos meus amigos do GIQ, Paulo Benício, João Batista, Daniel Barbosa, José Cláudio, David Sena e Wellington Brito pelos momentos de estudos, pesquisa, trabalho e descontração. E à recém ingressa ao grupo, Carol Timbó. Aos companheiros Clausson Rios, Aminadabe, Prof. Elvio César Girauldo. À Janaína Cruz pelos conselhos e apoio.

À Prof.^a Fátima e colegas do GPI, Iális, C. Janaína, Darby, Moziel, Karinne, Yuri e Tércio pelos momentos de descontração, paciência e compartilhamento da impressora. Aos meus contemporâneos de PET e, em especial, ao Prof. Paulo César Cortez.

Ao Prof. João César Moura Mota, Gilcélcio e demais professores e funcionários do Departamento de Engenharia de Teleinformática.

Aos professores e funcionários do Departamento de Engenharia Elétrica e colegas da Graduação Zé Iran, Rubens Guerra, Cybelle, Chico Rafael, Chico Fábio, Leonardo Olímpio, João Paulo Madeiro, Chico Ivan, Rui e outros mais.

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

Sumário

Lista de Figuras.....	9
Lista de Tabelas	12
Resumo	13
Abstract	14
Introdução	15
Capítulo 1.....	18
DISTRIBUIÇÃO QUÂNTICA DE CHAVES	18
1.1 Criptografia Clássica Vs. Criptografia Quântica	18
1.2 Princípio dos Protocolos de Distribuição Quântica de Chaves	22
1.2.1 Protocolo BB84.....	22
1.2.2 Protocolo B92.....	24
1.3 Codificação de Fase.....	25
1.4 Taxas de Transmissão da Chave e de Erro	26
Capítulo 2.....	30
ANÁLISE DE SISTEMAS ÓPTICOS DE DISTRIBUIÇÃO QUÂNTICA DE CHAVES COM PULSOS COERENTES FORTEMENTE ATENUADOS	30
2.1 Sistema de DQC Usando Interferômetro de Mach-Zehnder	30
2.2 Sistema de DQC Plug&Play Usando Interferômetro de Michelson com Espelhos de Faraday	33
2.3 Sistema de DQC Plug&play Usando Interferômetro Mach-Zehnder com Protocolo BB84.....	35
2.4 Sistema de DQC com Modulação de Fase Relativa entre Bandas Laterais	38
2.4.1 Modulação PM – PM	40
2.4.2 Modulação AM – AM.....	43
2.4.3 Modulação AM – PM (PM – AM)	45
2.4.4 Implementação de Sistema de DQC com BB84 modificado Usando Modulação de Fase Relativa entre Bandas Laterais com Sincronismo WDM.....	47
2.5 Implementação de um Sistema de DQC Polarimétrico de Alta Taxa de Transmissão.	50
2.6 Distribuição Quântica de Chaves com Interferômetro de Sagnac	53
2.7 Segurança de Sistemas de DQC Utilizando Estados Coerentes Fracos	55
Capítulo 3.....	57
SISTEMA DE DISTRIBUIÇÃO QUÂNTICA DE CHAVES COM MODULAÇÃO DE FASE RELATIVA ENTRE BANDAS LATERAIS USANDO MULTIPORTADORAS	57
3.1 Sistema de Distribuição Quântica de Chaves com Modulação de Fase Relativa entre Bandas Laterais Usando Multiportadoras.	57
Capítulo 4.....	62
RESULTADOS EXPERIMENTAIS DA IMPLEMENTAÇÃO DO PROTOCOLO DE DISTRIBUIÇÃO QUÂNTICA DE CHAVES B92	62
4.1 Detectores de Fótons Isolados – DFI	62
4.2 Resultados Experimentais do Sistema de DQC executando o Protocolo B92.....	69
Capítulo 5.....	76

ENCRIPÇÃO FÍSICA COM ESTADOS COERENTES MESOSCÓPICOS.....	76
5.1 Estados Coerentes.....	76
5.2 Parâmetros de Stokes	78
5.3 Descrição do Sistema de Encriptação Física com Estados Coerentes Mesoscópicos	82
Capítulo 6.....	88
CORREÇÃO DE ERRO QUÂNTICO APLICADA A ESTADOS COERENTES MESOSCÓPICOS COM ÓPTICA LINEAR.....	88
6.1 Sistema Ativo de Correção de Erro Quântico Aplicado a Estados Coerentes Mesoscópicos com Óptica Linear.	88
6.2 Sistema Passivo de Correção de Erro Quântico Aplicado a Estados Coerentes Mesoscópicos com Óptica Linear.	91
Capítulo 7.....	96
SISTEMAS HÍBRIDOS DE DISTRIBUIÇÃO QUÂNTICA DE CHAVES	96
7.1 Distinção de Estados Coerentes Polarizados: Número Médio de Fótons Versus Número de Bases.....	96
7.2 Sistema de Distribuição Quântica de Chaves Híbrido.....	98
7.3 Sistema de Híbrido de Autenticação Quântica de Mensagens Clássicas	99
Capítulo 8.....	101
RECEPTOR ÓPTICO PARA INSTRUMENTAÇÃO E COMUNICAÇÃO	101
8.1 Análise Teórica.....	101
8.2 Resultados Experimentais	105
8.3 Aplicação em Sistemas de Comunicações Ópticas	108
Capítulo 9	111
CONCLUSÕES E PERSPECTIVAS	111
REFERÊNCIAS	113

Lista de Figuras

Figura 1.1: Elementos básicos de um sistema de criptografia.....	19
Figura 1.2: Duas bases não-ortogonais. Os bits 0 e 1 são representados por estados ortogonais em qualquer uma das bases.....	20
Figura 1.3: Diagrama do fluxo de informação no algoritmo completo de distribuição quântica de chaves.....	21
Figura 1.4: Princípio da distribuição quântica de chaves, usando polarização da luz, de acordo com o protocolo BB84.....	23
Figura 1.5: Princípio da distribuição quântica de chaves conforme protocolo B92. A – atenuador variável, R – rotacionador de polarização e <i>PBS</i> – divisor de feixes por polarização.....	24
Figura 1.6: Configuração de um sistema interferométrico para DQC usando interferômetro de Mach-Zehnder.....	25
Figura 2.1: Implementação do sistema interferométrico de Mach-Zehnder para DQC. BS - acoplador óptico, PM - modulador de fase, DFI - detector de fótons isolados.	31
Figura 2.2: Interferômetro Plug&Play para DQC, protocolo B92, com espelhos de Faraday. FM - espelho de Faraday, $C_{1(2)}$ - acoplador, C – circulador.	33
Figura 2.3: Diagrama esquemático do sistema interferométrico Plug&Play com protocolo BB84.....	36
Figura 2.4: Aparato óptico usado para modulação de fase relativa entre bandas laterais. GNA – gerador de números aleatórios, PLO – oscilador de fase travada.	39
Figura 2.5: Espectro de frequência do pulso óptico na saída do modulador de Bob.....	42
Figura 2.6: Diagrama de um modulador de Mach-Zehnder.	43
Figura 2.7: Espectro de frequência do pulso óptico na saída do modulador de Bob para o caso AM-PM.....	47
Figura 2.8: Esquema experimental usado no sistema de DQC com sincronismo WDM. PG - gerador de pulsos, HF – Gerador de microondas, PHS - deslocador de fase, QPSK - modulador de fase, $AF_{s(1)}$ – atenuadores ópticos, <i>DL</i> - linha de atraso.	48
Figura 2.9: <i>NEP</i> versus comprimento de onda para FDAs de Si, Ge e de InGaAs.....	51
Figura 2.10: Comportamento teórico de FDAs de Si, Ge e de InGaAs em distâncias curtas para $\mu=0,1$ $\nu=10$ MHz, e dados da Tabela 2.7.	52
Figura 2.11: Esquema experimental usado na implementação do protocolo B92 de alta velocidade.....	53
Figura 2.12: Distribuição quântica de chaves tipo circular.	54
Figura 2.13: Distribuição quântica de chaves com interferômetro Sagnac.	54
Figura 3.1: Diagrama esquemático para o sistema de DQC com multiportadoras.....	57
Figura 4.1: FDA sob modo de extinção engatilhado (I) e trem de pulsos de gatilhos (II) ...	63
Figura 4.2: Pulso de gatilho experimental.	64
Figura 4.3: Esquema usado na caracterização do FDA.....	65
Figura 4.4: Pulso elétrico experimental que modula o laser.....	65

Figura 4.5: Pulso elétrico gerado na saída do fotodetector PIN devido à detecção do pulso óptico emitido pelo diodo laser.	67
Figura 4.6: Probabilidade de detecção no FDA_a (*) e FDA_b (o) versus atenuação.....	68
Figura 4.7: Detector de fótons isolados desenvolvido no LATIQ/UFC.....	68
Figura 4.8: Configuração óptica utilizada na implementação do sistema de DQC polarimétrico executando o protocolo B92.	69
Figura 4.9: Foto da configuração óptica utilizada na implementação do sistema de DQC polarimétrico executando o protocolo B92.	70
Figura 4.10: Tela do software que controla o sistema de DQC.....	70
Figura 4.11: Probabilidade de detecção no DFI_a quando foram enviados apenas bits 1 (*) e apenas bits 0 (.) com o conjunto de parâmetros $V_g=3,43V$, $\tau_g=6,825ns$, $V_{FDA}=40,5V$ e $T\approx 45^\circ C$. $P_{Da}=0,04419$ e $NEP_a = 23,075 \times 10^{-13} J/\sqrt{Hz}$	71
Figura 4.12: Probabilidade de detecção no DFI_b quando foram enviados apenas bits 0 (.) e apenas bits 1 (*) com o conjunto de parâmetros $V_g=3,43V$, $\tau_g=6,825ns$, $V_{FDA}=40,5V$ e $T\approx 45^\circ C$. $P_{Da}=0,05005$ e $NEP_b = 12,278 \times 10^{-13} J/\sqrt{Hz}$	72
Figura 4.13: Taxa de erro versus atenuação quando são enviados apenas bits 0 (o) e apenas bits 1 (*).	73
Figura 4.14: Probabilidade de detecção no DFI_a (o), DFI_b (*) e a taxa de erro (\square) quando uma seqüência aleatória de bits é enviada por Alice.	73
Figura 4.15: Probabilidade de detecção no DFI_a quando são enviados apenas bits 0 (*) e apenas bits 1 (.) com o conjunto de parâmetros $V_g=3,43V$, $\tau_g=9ns$, $V_{FDA}=41V$ e $T\approx 45^\circ C$. $P_{Da}=0,08702$ e $NEP_a=14,099 \cdot 10^{-13} J/Hz^{1/2}$	74
Figura 4.16: Probabilidade de detecção no DFI_b quando forma enviados apenas bits 0 (*) apenas bits 1 (.) com o conjunto de parâmetros $V_g=3,43V$, $\tau_g=9ns$, $V_{FDA}=41V$ e $T\approx 45^\circ C$. $P_{Db}=0,10548$ e $NEP_b=8,278 \cdot 10^{-13} J/Hz^{1/2}$	75
Figura 4.17: Probabilidade de detecção no DFI_a (*), DFI_b (.) e a taxa de erro (\square) quando uma seqüência aleatória de bits é enviada por Alice com os parâmetros $V_g=3,43V$, $\tau_g=9ns$, $V_{FDA}=41V$ e $T\approx 45^\circ C$. $P_{Da}=0,08702$ e $NEP_a=14,099 \times 10^{-13} J/\sqrt{Hz}$. $P_{Db}=0,10548$ e $NEP_b = 8,278 \times 10^{-13} J/\sqrt{Hz}$	75
Figura 5.1: Distribuição do número de fótons $p(n)$ versus número de fótons n para estados coerentes com $ \alpha ^2=0,1$ (o), $ \alpha ^2=1$ (*) e $ \alpha ^2=10$ (x).	77
Figura 5.2: Diagrama do vetor de Stokes clássico (a) e quântico (b) mapeados na esfera de Poincaré. A bola no final do vetor representa o ruído quântico nos operadores \hat{S}_1 , \hat{S}_2 e \hat{S}_3	80
Figura 5.3: Esquema básico para implementação de protocolos de comunicação quântica usando estados coerentes mesoscópicos. A - amplificador óptico com ganho G, V - sinal elétrico para modulação dos pulsos mesoscópicos.	83
Figura 5.4: Círculo de codificação para ângulos de fase ϕ_k para $M=1$ a $M=5$. Cada valor de k especifica uma base de dois estados, defasados de π , que representam o bit 0 (o) e o bit 1 (•).	83
Figura 6.1: Sistema de comunicação quântica usando estados coerentes mesoscópicos e esquema ativo de correção de erro. PC - célula de Pockels.	89

Figura 6.2: Esquema passivo para correção de erros. BS – Acoplador óptico balanceado..	92
Figura 6.3: Sistema de comunicação quântica usando estados coerentes mesoscópicos e esquema passivo de correção de erro. E.O.S – chave eletro-óptica.	94
Figura 7.1: Medição da polarização de um pulso coerente multifótons usando a força bruta.	97
Figura 7.2: Sistema de DQC híbrido que executa o protocolo BB84 polarimétrico.	99
Figura 7.3: Protocolo de autenticação quântica de mensagens clássicas.	100
Figura 8.1: Circuito eletrônico do receptor óptico.	102
Figura 8.2: Modelo AC para o receptor óptico.	102
Figura 8.3: Modelo AC com ruído para o receptor óptico.	104
Figura 8.4: Esquema usado nos testes do receptor óptico.	106
Figura 8.5: Potência de saída do laser [mW] versus corrente de injeção do laser [mA] para dois valores de temperaturas: (I) 10kΩ e (II)5kΩ.	106
Figura 8.6: Tensão de saída do receptor óptico versus potência óptica incidente com laser operando na temperatura de 10kΩ: (1) PIN FGA04 e (2) FDA C30645E.	107
Figura 8.7: Tensão de saída do receptor óptico, V_o , versus a temperatura do laser e corrente de injeção, usando o fotodiodo PIN FGA04.	107
Figura 8.8: Responsividade \mathfrak{R}_e [V/mW] versus potência de saída do laser para o fotodiodo FGA04 para as temperaturas $T_L=10k\Omega$ (o) e $T_L=5k\Omega$ (*).	108
Figura 8.9: Circuito que fornece um pulso TTL de largura controlável na saída para cada avalanche.	109
Figura 8.10: Pulso elétrico que modula o diodo laser (1) e sinal elétrico na entrada não-inversora amplificador operacional (2).	110
Figura 8.11: Pulso TTL na saída do detector (1) e o sinal amplificado na saída do amplificador operacional (2).	110

Lista de Tabelas

Tabela 1.1: Implementação do protocolo BB84 com codificação de fase.	26
Tabela 2.1: Resultados experimentais do sistema Plug&Play com interferômetro de Michelson usando espelhos de Faraday.....	35
Tabela 2.2: Medidas de visibilidade do sistema Plug&Play.	38
Tabela 2.3: Resultados do sistema Plug&Play para diferentes enlaces de fibra óptica. K é o comprimento inicial da chave.....	38
Tabela 2.4: Implementação do protocolo B92 para sistema PM-PM.....	42
Tabela 2.5: Implementação do protocolo BB84 para sistema AM-PM.	46
Tabela 2.6: Comparação entre os sistemas já realizados e, em negrito, está o descrito nesta seção.	50
Tabela 2.7: Parâmetros típicos de FDAs de Si, Ge e de InGaAs disponíveis comercialmente.....	51

Resumo

Nesta dissertação é realizado um estudo sobre implementações de distribuição quântica de chaves (DQC) em redes ópticas. Inicialmente, é feita uma revisão da teoria da distribuição quântica de chaves com fótons isolados e de algumas implementações com estados coerentes fortemente atenuados, bem como a revisão de um sistema óptico para encriptação física de mensagens utilizando estados coerentes mesoscópicos. Em seguida, é analisada a utilização de um sistema de correção de erros para o sistema de encriptação física usando estados coerentes mesoscópicos, e são propostos dois novos esquemas de distribuição quântica de chaves. O primeiro é a possível implementação de um sistema híbrido, isto é, utilizando estados coerentes fortemente atenuados e estados coerentes mesoscópicos, para DQC e autenticação quântica de mensagens clássicas. O segundo é uma implementação de um sistema de DQC baseado em modulação de fase relativa entre bandas laterais de frequência, utilizando duas portadoras de RF e moduladores de amplitude em Alice e fase em Bob. Posteriormente, é detalhada a realização experimental de um sistema de DQC, simples e didática, usando estados de polarização de pulsos coerentes fortemente atenuados que executa o protocolo B92. Por fim, é feita a caracterização teórica e experimental de um receptor óptico para uso em comunicações ópticas.

Abstract

In this dissertation it is realized a study about quantum key distribution (QKD) in optical networks. Initially, a review of the theory of quantum key distribution and some of its implementations with strongly attenuated coherent states, as well a review of an optical system for physical encryption using mesoscopic coherent states are realized. Following, it is analyzed the use of an error correction scheme in the physical encryption system, and two new schemes for quantum key distribution are proposed. The first is a possible implementation of a hybrid system, that is, using weak and mesoscopic coherent states, for QKD and quantum authentication of classical messages. The second is an implementation of a QKD system based on relative phase modulation of sidebands frequency, using two RF carriers and an amplitude modulator in Alice and a phase modulator in Bob. After, an experimental realization of a simple QKD setup using polarization states of strongly attenuated coherent states for B92 protocol is presented. At last, it is realized an experimental characterization of an optical receiver for optical communication applications.

Introdução

Com a expansão da internet, aumentou também o volume de operações realizadas por seu intermédio tais como: troca de informações secretas entre empresas, instituições militares, transações financeiras e comerciais (comércio eletrônico), governo digital, dentre outras. Sendo assim, um dos pontos mais relevantes para as modernas redes de comunicação é a garantia de que os dados que por elas trafegam estejam totalmente seguros contra possíveis tentativas de espionagem por usuários não autorizados. Para garantir tal segurança, são usados algoritmos de encriptação de dados cuja segurança é garantida pela complexidade matemática em fatorar números primos de valor muito grande. No entanto, em 1994, Shor descreveu um algoritmo que, quando executado por um *computador quântico*, seria capaz de resolver problemas de fatoração em tempo muito mais hábil que os computadores clássicos. Portanto, com a evolução dos sistemas de computação e, futuramente, com a implementação do computador quântico, a segurança de sistemas que utilizam autenticação por chave pública está seriamente comprometida.

Por outro lado, os esquemas de criptografia que utilizam o protocolo “*one-time pad*” são considerados os únicos incondicionalmente seguros. Nesse caso, os usuários devem manter um processo dinâmico de descarte da chave recém utilizada e de compartilhamento de uma nova chave a fim de garantir segurança absoluta no processo. Surge então uma outra questão: qual a garantia de que a troca da chave não será monitorada por algum intruso? Uma das principais características dos atuais sistemas de informação é que eles operam dentro do domínio da física clássica. Cada bit de informação pode ser completamente descrito por variáveis clássicas tais como o nível de tensão na entrada de um transistor ou microprocessador, ou a carga armazenada em um capacitor. Com os avanços da mecânica quântica no século XX, que possibilitou ao homem explicar alguns fenômenos para os quais a teoria da física clássica é considerada incompleta, demonstrou-se que a informação também poderia ser processada e transmitida por sistemas físicos que só podiam ser completamente descritos e compreendidos pela mecânica quântica. Em particular, em 1983, Wiesner publicou um trabalho mostrando que as propriedades da mecânica quântica podiam ser usadas em criptografia. Em 1984, C. H. Bennet, da IBM, e

G. Brassard, da Universidade de Montreal, propuseram o primeiro algoritmo de distribuição de chaves garantido pelas propriedades da mecânica quântica, conhecido como BB84. Surgia então uma nova e fascinante área de conhecimento: a teoria da informação quântica.

A informação quântica divide-se, basicamente, em duas sub-áreas: computação e comunicação quântica. A primeira é a que traz mais desafios para físicos e engenheiros, pois, embora sua teoria já esteja bem alicerçada, sua realização ainda se resume a sistemas bastante simples sem nenhum tipo de aplicação prática até o momento. Isto é normal, pois esta nova teoria requer também novas formas de trabalhar na escala atômica que é algo muito delicado e que exige o desenvolvimento e o aprimoramento de novas técnicas capazes de manipular fótons, elétrons, átomos e moléculas isoladamente. Em relação à comunicação quântica, esta é a que apresenta os resultados experimentais mais expressivos, estando a distribuição quântica de chaves (DQC) e a teleportação quântica em estágios bem avançados, existindo sistemas comercialmente disponíveis que executam protocolos de DQC.

Nesse contexto, o objetivo desse trabalho é analisar os principais sistemas experimentais já realizados e mostrar os resultados experimentais da implementação de um sistema óptico de distribuição quântica de chaves, desenvolvido no LATIQ/DETI, executando o protocolo B92.

Esta dissertação está dividida em nove capítulos. No primeiro capítulo, é apresentada uma revisão sobre distribuição quântica de chaves. São mostrados os princípios de operação dos protocolos BB84 e B92, e a análise dos principais parâmetros de desempenho como taxa de erro e taxa de transmissão.

No Capítulo 2 são analisados os principais sistemas ópticos de distribuição quântica de chaves, destacando o sistema “Plug&Play” e o que utiliza modulação de fase relativa entre bandas laterais de frequência.

No Capítulo 3 é proposto um sistema que usa modulação de fase relativa entre bandas laterais multiportadoras para implementação paralela de dois protocolos BB84.

No Capítulo 4 são apresentados os resultados experimentais da implementação de um sistema óptico de distribuição quântica de chaves, desenvolvido no LATIQ/DETI, executando o protocolo B92.

No Capítulo 5 é feita, primeiramente, uma revisão sobre estados coerentes e polarização quântica. Em seguida, é mostrado o protocolo de encriptação física de mensagens que utiliza estados coerentes mesoscópicos e a análise dos principais aspectos de segurança.

No Capítulo 6 é discutida a aplicação de um esquema de correção de erro quântico, ativo e passivo, usando óptica linear empregado ao sistema do Capítulo 5 para estados de polarização.

No Capítulo 7 é proposta a aplicação do sistema que usa estados coerentes mesoscópicos na implementação de um sistema híbrido de DQC e de autenticação quântica de mensagens clássicas.

No Capítulo 8 é mostrada a caracterização teórica e experimental de um detector óptico usado para instrumentação e comunicação, e que foi usado como ferramenta para obtenção do número médio de fótons no experimento do Capítulo 4.

Por fim, as conclusões e as perspectivas de futuros trabalhos são apresentadas no Capítulo 9.

Capítulo 1

DISTRIBUIÇÃO QUÂNTICA DE CHAVES

Neste capítulo é apresentado como a distribuição quântica de chaves (DQC) proporciona segurança incondicional na distribuição de chaves. São discutidos os protocolos de DQC BB84 e B92, e mostrados os principais parâmetros de medição de desempenho em sistemas de DQC em redes ópticas.

1.1 Criptografia Clássica Vs. Criptografia Quântica

Basicamente, criptografia é a técnica de enviar mensagens secretamente de tal forma que apenas os usuários legítimos da comunicação sejam capazes de decifrá-la. A ideia é criar um criptograma da mensagem com o auxílio de uma chave criptográfica e que, sem a chave correta, seja muito difícil para um usuário não autorizado recuperar a mensagem original a partir do criptograma em tempo hábil. Em criptografia clássica, os principais métodos de distribuição de chaves são: o simétrico e o assimétrico ou de chave pública [1].

No método assimétrico, um usuário, denotado por *Bob*, gera uma chave pública a partir de uma chave secreta que só ele detém e a divulga para um outro usuário interessado em transmitir mensagem para ele, denotado por *Alice*. Quando Alice enviar uma mensagem codificada com a chave pública que Bob divulgou, apenas ele será capaz de lê-la, pois somente ele possui a chave secreta correta. A segurança desse método está fundamentada na complexidade matemática e computacional necessária para decifrar o código. Portanto, ela está ameaçada pelo avanço nas implementações de algoritmos de fatoração mais rápidos e do computador quântico.

No método simétrico, os usuários devem compartilhar a mesma chave secreta escolhida de forma totalmente aleatória. Como mostrado na Figura 1.1, Alice codifica sua mensagem (m) pela adição da chave secreta gerada aleatoriamente (c) que ela detém e envia

o criptograma ($E[m,c]$) para Bob. Como ele tem conhecimento da chave usada por Alice, Bob subtrai a chave do criptograma e obtém a mensagem original. Esse método, conhecido como *one-time pad*, é o único considerado totalmente seguro. A razão de sua segurança é que, como a mensagem codificada é formada a partir da operação *XOR* da mensagem a ser transmitida com a chave aleatória, o criptograma resultante torna-se também igualmente aleatório, não contendo nenhuma informação coerente para quem não possua a chave. Vale ressaltar que Alice e Bob devem usar a mesma chave apenas uma vez. O reuso da chave pode possibilitar para Eva um ganho de informação parcial sobre a mensagem. Portanto, para que a segurança ainda permaneça garantida, é necessário que os usuários legítimos permaneçam em um processo constante de troca de chaves criptográficas secretas aleatórias.

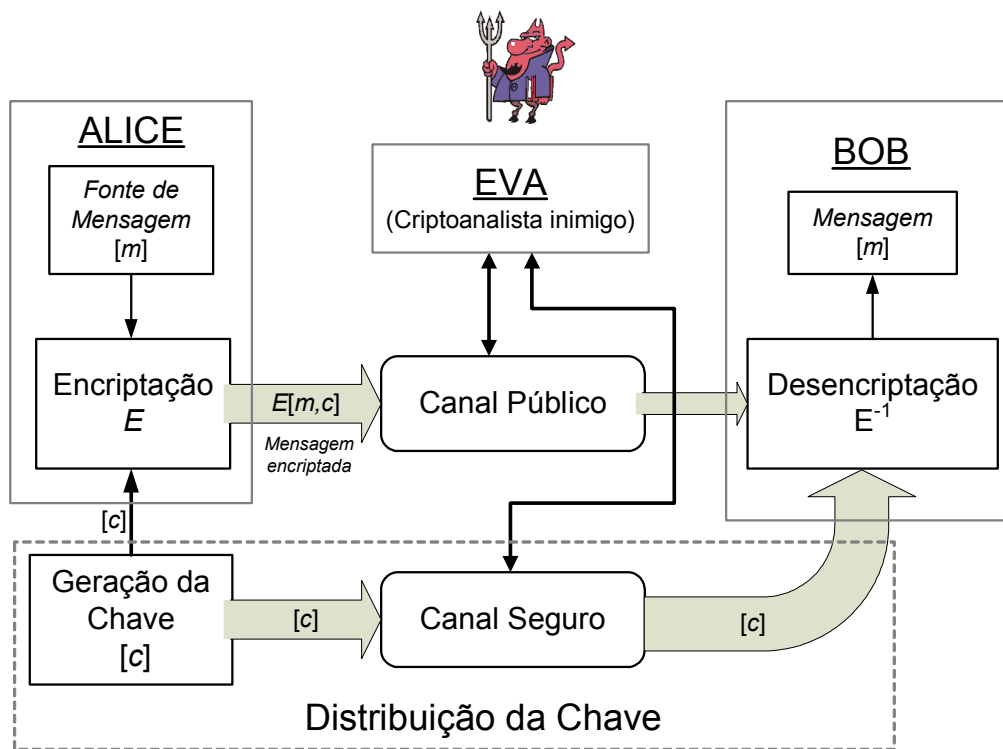


Figura 1.1: Elementos básicos de um sistema de criptografia.

No entanto, o principal problema dos sistemas criptográficos é a garantia de que a chave será distribuída entre os usuários legítimos de forma segura. Convencionalmente, como está mostrado na Figura 1.1, é estabelecido um canal seguro entre transmissor e receptor que torna difícil, mas não impossível para um terceiro usuário não autorizado

adquirir informações sobre a chave. Portanto, enquanto a segurança dos métodos criptográficos clássicos está ameaçada pelos avanços tecnológicos e dos algoritmos matemáticos, a física quântica aparece como uma solução que possibilita a segurança incondicional na transmissão da chave.

Distribuição quântica de chaves é a técnica que permite a troca segura de uma sequência aleatória de bits, usada como chave em um algoritmo de criptografia [2,3]. A segurança dos protocolos usados é garantida pelos seguintes fatores que são derivados dos postulados da mecânica quântica:

- A escolha de uma codificação adequada em uma propriedade quântica;
- A indivisibilidade de um quantum;
- A impossibilidade de fazer uma cópia perfeita de um estado quântico (não é possível discriminar estados quânticos não ortogonais com total precisão), conforme ilustrado na Figura 1.2.

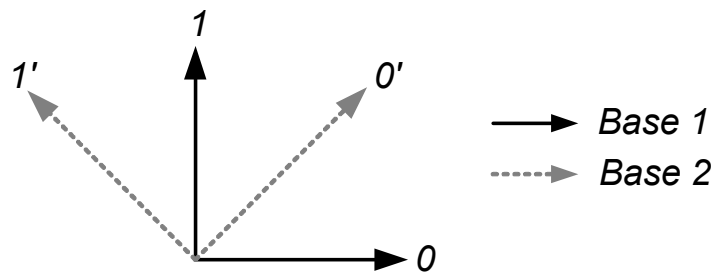


Figura 1.2: Duas bases não-ortogonais. Os bits 0 e 1 são representados por estados ortogonais em qualquer uma das bases.

Em física clássica, a medição de uma grandeza não altera o valor da mesma. Semelhantemente, em comunicação clássica, o bit de informação é codificado em bilhões de fótons ou elétrons, por exemplo. Assim, é sempre possível desviar uma parte do sinal e executar uma medição nele sem ser percebido. Por outro lado, no sistema de DQC, cada bit de informação é codificado em uma propriedade quântica de um fóton. Uma propriedade quântica de dois estados possíveis, como a polarização da luz, por exemplo, é chamada de *bit quântico – qubit* [4]. Um fóton não pode ser dividido (indivisibilidade de um quantum),

nem ter sua informação copiada (teorema da não clonagem). No caso de fótons, os estados quânticos utilizados para portar a informação podem ser a polarização, como mencionado anteriormente, ou a fase. A diferença entre bits e *qubits* é que esses últimos podem se apresentar em uma superposição dos dois estados que formam a base, $|q\rangle = a|0\rangle + b|1\rangle$, sendo que nesse caso o estado $|q\rangle$ é $|0\rangle$ e $|1\rangle$ ao mesmo tempo. Quando uma medição é feita nesse estado, o resultado será $|0\rangle$ com probabilidade $|a|^2$, ou $|1\rangle$ com probabilidade $|b|^2$. Os estados $|0\rangle$ e $|1\rangle$ são ortogonais e, portanto, perfeitamente distinguíveis em uma medição. A informação quântica deve ser enviada por um canal quântico, ou seja, um canal capaz de preservar os estados quânticos dos fótons durante a transmissão.

É importante ressaltar que a física quântica não impede os ataques de espionagem. Ela apenas possibilita detectar a presença de um intruso. Quando uma alta taxa de erro for encontrada, a chave é simplesmente descartada e os usuários repetem o procedimento para gerar uma nova chave. Um exemplo do mapa de fluxo de informação em DQC, da transmissão dos bits da seqüência aleatória gerada por Alice até o estabelecimento de uma chave secreta comum a Bob e Alice é mostrado na Figura 1.3.

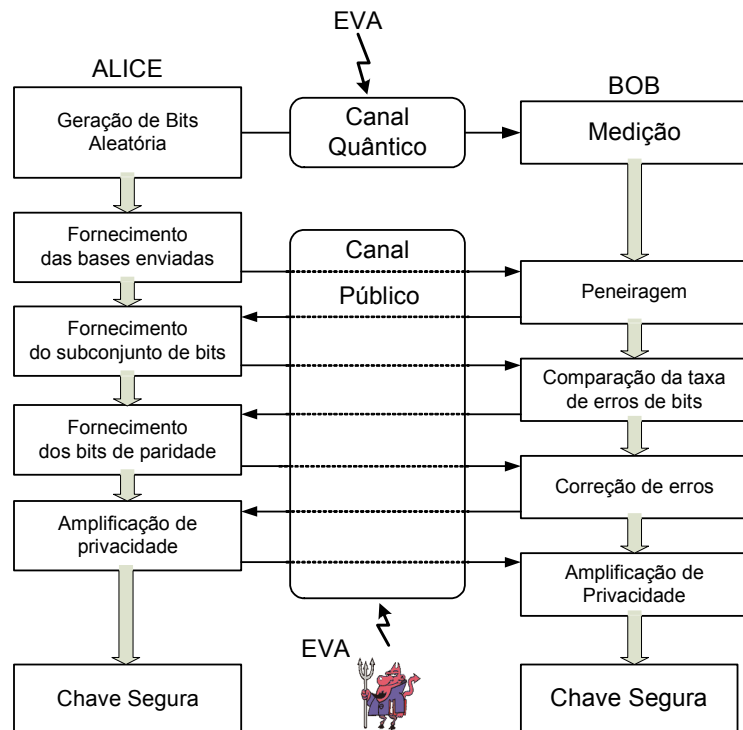


Figura 1.3: Diagrama do fluxo de informação no algoritmo completo de distribuição quântica de chaves.

Vale destacar que a geração da chave bruta (a seqüência aleatória de bits), deve ser muito maior que a chave final para a encriptação. A amplificação de privacidade envolve o sacrificio de bits através da aplicação, na chave corrigida, de uma função digital não linear. Tais funções digitais não lineares possuem número de bits de saída inferior ao número de bits de entrada e são conhecidas como funções *Hash*. A chave final é obtida após esta etapa.

1.2 Princípio dos Protocolos de Distribuição Quântica de Chaves

Os dois principais protocolos de DQC em sistemas interferométricos são descritos nesta seção. O primeiro destes protocolos foi proposto em 1984 por Charles H. Bennett, da IBM e Gilles Brassard, da Universidade de Montreal, por isso motivo chama-se BB84. Ele consiste de um esquema de quatro estados quânticos que originalmente se baseou em codificação de polarização, mas pode também ser utilizado com codificação em fase. No caso do B92, proposto por Bennett em 1992, trata-se de uma versão do BB84 usando apenas dois estados não ortogonais entre si.

1.2.1 Protocolo BB84

O protocolo BB84, Figura 1.4 [3], usa quatro estado quânticos que constituem duas bases, ou seja, dois pares de estados ortogonais. Inicialmente, Alice envia uma seqüência de fótons, com polarização linear $\{|H\rangle, |V\rangle\}$ ou diagonal $\{|+\rangle, |-\rangle\}$, aleatoriamente escolhida. Esta seqüência e a janela de tempo de cada qubit são armazenadas por Alice. Em seguida, Bob mede a polarização de cada fóton da seqüência e também grava o resultado suas medições bem como a janela de tempo de recebimento de cada fóton. Depois da transferência de um número suficiente de fótons, Bob anuncia, pelo canal público, a sua seqüência de bases usadas na detecção, mas não o resultado obtido. Alice compara esta seqüência com a sua e informa-o em que posições as bases selecionadas por ambos são diferentes. Os bits correspondentes são descartados na seqüência de ambos. Os bits restantes formam uma chave bruta. A chave obtida depois da reconciliação das bases é chamada de chave peneirada (*sifted key*).

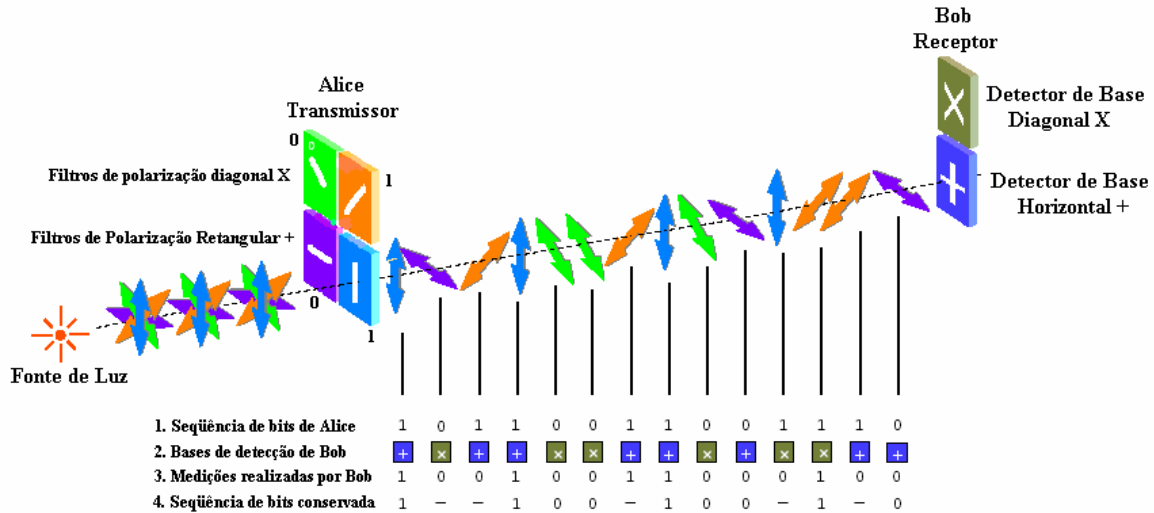


Figura 1.4: Princípio da distribuição quântica de chaves, usando polarização da luz, de acordo com o protocolo BB84.

Na terceira etapa do protocolo, Alice e Bob selecionam aleatoriamente um subconjunto da chave bruta e compara-o através do canal público, a fim de avaliar a taxa de erro da comunicação. Caso a comunicação tenha sido interceptada por Eva, ela introduzirá erro nas medições de Bob. A probabilidade de Eva causar um erro na comunicação entre Alice e Bob é de 25%, 50% de Eva medir o *qubit* em uma base diferente da usada por Alice e Bob e 50% de probabilidade do bit enviado por Eva causar um erro em Bob. Assim, quando Eva estiver presente, na ausência de ruídos inerentes ao sistema, cerca de $\frac{1}{4}$ dos bits de Alice e Bob estarão errados, revelando facilmente sua presença como intrusa no processo de distribuição da chave. Sob estas condições, a chave será descartada e o processo reiniciado.

Na última etapa do protocolo, considerando que não foi detectada a presença de intruso na transmissão pelo canal quântico, existirão, na prática, alguns erros na chave peneirada. Estes erros devem ser removidos por métodos clássicos de correção de erros, o que poderá reduzir o comprimento da chave. Se o protocolo de correção de erro descarta os bits errados, o protocolo de DQC acaba aqui. No entanto, se os bits errados da chave são corrigidos, alguma informação é sempre vazada para Eva durante o processo de correção. Assim, objetivando aumentar a privacidade, Alice e Bob aplicam uma função *Hash* em suas chaves. A aplicação dessa função embaralha os bits da chave de tal modo que, mesmo que inicialmente duas chaves difiram em apenas um bit, após a aplicação de tal função, as

chaves finais apresentam, aproximadamente, 50% dos valores dos bits diferentes. A chave restante após o processo de amplificação de privacidade pode finalmente ser usada com total confiança para codificar uma mensagem usando algoritmos *one-time pad*. Por motivo de segurança, é comum tomar a taxa de erro como sendo completamente atribuída a um intruso.

1.2.2 Protocolo B92

O protocolo B92, Figura 1.5, usa dois estados quânticos não ortogonais. Inicialmente, Alice envia uma seqüência de fótons, com polarização $|H\rangle$ para o bit 0 e $|\pi/4\rangle$ para o bit 1, escolhida aleatoriamente. Bob, por sua vez, escolhe aleatoriamente se rotaciona ou não a polarização do fóton que chega ao seu aparato óptico. Assim, com base em medições conclusivas, toda vez que há uma contagem nos detectores D_0 ou D_1 , Bob conclui que o bit enviado por Alice foi ‘0’ ou ‘1’, respectivamente. Por outro lado, qualquer contagem nos detectores D_2 , Bob não tem certeza sobre qual bit Alice quis enviar. Além disso, no processo de reconciliação, Bob avisa para Alice os instantes em que houve detecção e, naqueles em que não houve nada, eles simplesmente descartam esse bits e obtêm a chave peneirada. Com essa chave peneirada, Alice e Bob aplicam os mesmos métodos de detecção de intruso, com base no aumento da taxa de erro do sistema, correção de erros e amplificação de privacidade como é feito para o BB84.

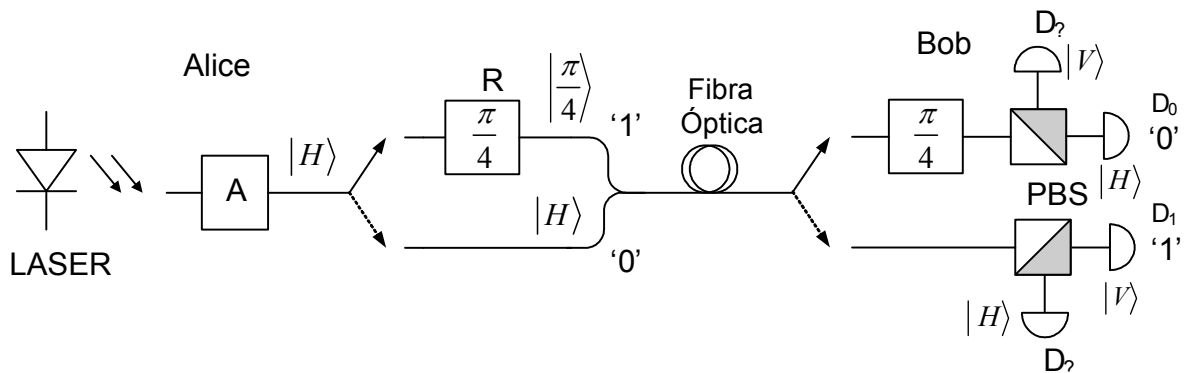


Figura 1.5: Princípio da distribuição quântica de chaves conforme protocolo B92. A – atenuador variável, R – rotacionador de polarização e PBS – divisor de feixes por polarização.

1.3 Codificação de Fase

Sistemas baseados em codificação de polarização apresentam um sério problema para transmissão por fibra óptica em longa distância. O efeito de dispersão de modos de polarização faz com que a polarização da luz no interior da fibra varie aleatoriamente ao longo da fibra. Para tais sistemas, uma possível solução é o uso de controle ativo de compensação da polarização. Esta opção é complexa, principalmente operando no regime quântico. A solução mais viável é usar sistemas com codificação de fase.

A configuração conceitual de um sistema interferométrico para distribuição quântica de chaves é mostrada na Figura 1.5 [1]. Trata-se de um interferômetro de Mach-Zehnder de fibra óptica composto por dois acopladores ópticos balanceados (50/50) e com um modulador de fase em cada braço de mesmo comprimento. Para cada fóton emitido por Alice, proveniente do diodo laser (LD), as probabilidades do mesmo emergir do interferômetro nas saídas ‘0’ e ‘1’ de C_2 dependem da diferença de fase $\phi_A - \phi_B$.

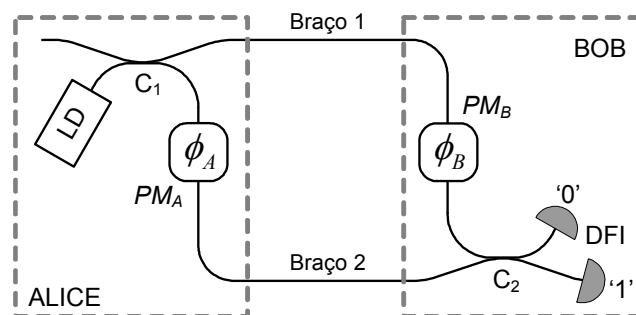


Figura 1.6: Configuração de um sistema interferométrico para DQC usando interferômetro de Mach-Zehnder.

Para executar o protocolo BB84, Alice pode usar um dos quatro deslocamentos de fases ($0, \pi/2, \pi, 3\pi/2$), codificando o bit 0 com os deslocamentos ϕ_A de 0 rad ou $\pi/2$ rad, e π rad ou $3\pi/2$ para o bit 1. Do outro lado, Bob apenas usa duas fases, ϕ_B , 0 ou $\pi/2$. Os fótons registrados pelo detector DFI ‘0’ são considerados bits 0 e os detectados em DFI ‘1’, como bits 1. As intensidades da luz nas saídas ‘0’ e ‘1’ de C_2 são, respectivamente [1]

$$I_0 = \bar{I} \cos^2\left(\frac{\phi_A - \phi_B}{2}\right) \quad (1.1)$$

$$I_1 = \bar{I} \left[\sin^2\left(\frac{\phi_A - \phi_B}{2}\right) \right], \quad (1.2)$$

em que \bar{I} é a intensidade da luz emitida por Alice. Quando a luz emitida por ela contém, idealmente, apenas um fóton, (1.1) e (1.2) representam as probabilidades, respectivamente, de o fóton ser registrado nos detectores ‘0’ e ‘1’. Com bases nestas equações, Bob será capaz de realizar medições precisas quando $\phi_A - \phi_B$ for 0 rad ou π rad. No entanto, quando a diferença for $\pi/2$ rad ou $3\pi/2$ rad, o fóton será guiado, com 50% de chance, para qualquer um dos dois detectores, sendo que essas detecções são descartadas conforme determinação do protocolo BB84. Os possíveis resultados estão mostrados na Tabela 1.1.

<i>Alice</i>		<i>Bob</i>		
<i>Bit</i>	ϕ_A	ϕ_B	$\phi_A - \phi_B$	<i>Bit</i>
0	0	0	0	0
0	0	$\pi/2$	$3\pi/2$?
1	π	0	π	1
1	π	$\pi/2$	$\pi/2$?
0	$\pi/2$	0	$\pi/2$?
0	$\pi/2$	$\pi/2$	0	0
1	$3\pi/2$	0	$3\pi/2$?
1	$3\pi/2$	$\pi/2$	π	1

Tabela 1.1: Implementação do protocolo BB84 com codificação de fase.

1.4 Taxas de Transmissão da Chave e de Erro

Antes de ser detalhado o funcionamento de alguns dos principais sistemas ópticos para DQC, é importante apresentar os principais parâmetros de medição de desempenho considerados em qualquer sistema de comunicação que são: a taxa de transmissão de dados e a taxa de erro de bits.

O *QBER*, taxa de erros de bits quânticos, é definido pela razão entre o número de bits errados ($N_{errados}$) e o número total de bits enviados e pode ser expresso, também, em termos de taxa como sendo [1]:

$$QBER = \frac{N_{errados}}{N_{errados} + N_{corretos}} = \frac{R_{erro}}{R_{erro} + R_{sift}} \approx \frac{R_{erro}}{R_{sift}}. \quad (1.3)$$

A taxa R_{sift} corresponde aos casos em que Alice e Bob usaram a mesma base do protocolo e equivale à metade da taxa bruta de bits recebidos por Bob, R_{raw} . A relação entre elas é dada por

$$R_{sift} = \frac{1}{2} R_{raw} = \frac{1}{2} \mu \eta_B t_{canal} f, \quad (1.4)$$

em que μ é o número médio de fótons por pulso que Alice envia a Bob, η_B é a eficiência de detecção de Bob, f é a taxa de transmissão do laser e t_{canal} é a transmissividade do canal de comunicação entre Alice e Bob.

Existem basicamente três contribuições para a taxa de erro R_{erro} [1]. A primeira delas é devida aos fótons que são desviados para detectores errados devido, por exemplo, à interferência não perfeita. A taxa R_{opt} é dada pelo produto entre R_{sift} e a probabilidade p_{opt} de um fóton ir para o detector errado:

$$R_{opt} = R_{sift} \times p_{opt} = \frac{1}{2} f \mu \eta_B t_{canal} \times p_{opt}. \quad (1.5)$$

A segunda contribuição, R_{det} , é devido às contagens de escuro nos detectores. Essa taxa é independente da taxa de bits. Só são consideradas contagens de escuro geradas durante a janela de tempo em que a chegada de um fóton é esperada. Ela é dada por [1]

$$R_{det} = \frac{1}{2} \frac{1}{2} f p_{esc} n, \quad (1.6)$$

em que p_{esc} é a probabilidade de registrar uma contagem de escuro e n é o número de detectores usados no sistema de detecção do receptor. Os dois fatores $\frac{1}{2}$ estão relacionados ao fato de uma contagem de escuro ter 50% de chance de acontecer quando Alice e Bob escolhem bases diferentes (sendo eliminado durante o processo de reconciliação) e 50% de chance de ocorrer no detector correto. A terceira contribuição, R_{acc} , só é considerada em sistemas que utilizam fótons entrelaçados, o que não é o caso dos sistemas apresentados nessa dissertação. Basicamente, ela ocorre quando fótons de pares diferentes que chegam na mesma janela temporal não são necessariamente do mesmo estado. Ela é dada por

$$R_{acc} = \frac{1}{2} \frac{1}{2} p_{acc} f t_{canal} \eta_B n, \quad (1.7)$$

em que P_{acc} é a probabilidade de encontrar um segundo par dentro de uma janela de tempo, dado que um já foi criado. O $QBER$ pode ser expresso, então, por

$$\begin{aligned} QBER &= \frac{R_{opt} + R_{det} + R_{acc}}{R_{sift}} = p_{opt} + \frac{p_{esc} n}{2 t_{canal} \eta_B \mu} + \frac{p_{acc}}{2 \mu} = \\ &= QBER_{opt} + QBER_{det} + QBER_{acc} \end{aligned} \quad (1.8)$$

O $QBER_{opt}$ é dependente da distância entre os usuários e da taxa de transmissão. Ele depende, basicamente, do contraste das franjas de interferência (em sistemas por codificação de fase) ou do contraste de polarização. Sendo assim, ele pode ser considerado como uma medida da qualidade do balanceamento óptico do sistema. Os esforços técnicos necessários para obter e manter um determinado $QBER_{opt}$ é um critério importante para avaliação de diferentes esquemas de DQC. Em sistemas de curta distância que usam polarização, é relativamente fácil alcançar um contraste de polarização de 100:1, correspondendo a $QBER_{opt}$ de 1%. Já em sistemas interferométricos, efeitos como despolarização e desalinhamento de polarização deterioram a visibilidade V do interferômetro, ou seja, a capacidade de distinguir entre ocorrência de interferência construtiva e destrutiva. Em esquemas que utilizam codificação em fase, o $QBER_{opt}$ e a visibilidade de franjas estão relacionadas por [1]

$$QBER_{opt} = \frac{1-V}{2}. \quad (1.9)$$

Por exemplo, uma visibilidade de 98% equivale a um $QBER_{opt}$ de 1%. Um dos principais esquemas ópticos que mantém um valor de visibilidade razoavelmente alto e estável são os sistemas “*Plug&Play*” que serão detalhados no próximo capítulo. O $QBER_{det}$, que é devido à taxa de contagem de escuro dos detectores de fótons isolados, é o um fator determinante em transmissão de longa distância. Uma vez que as perdas da fibra já atingiram os limites físicos, a melhoria de desempenho dos sistemas de DQC depende crucialmente do desenvolvimento de melhores detectores. O limite teórico para a criação de chaves absolutamente segura é para $QBER$ inferior a 15%. A fração de bits perdidos pelo processo de reconciliação (correção de erro por descarte de bits), r_{ce} , em função do $QBER$ é dado por [3,4]:

$$r_{ce} = \left(\frac{7}{2} - \log_2(QBER) \right) QBER. \quad (1.10)$$

A taxa de compressão resultante da amplificação de privacidade, r_{ap} , é [3]

$$r_{ap} = \log_2(1 + 4QBER - 4QBER^2). \quad (1.11)$$

Por fim, a taxa de transmissão efetiva é dada por [3]:

$$R_{ef} = (1 - r_{ce})(1 - r_{ap})R_{Bruta}. \quad (1.12)$$

Encerrado este capítulo introdutório sobre a teoria da distribuição quântica de chaves, serão mostrados, no próximo capítulo, os principais sistemas ópticos de DQC usando fótons isolados.

Capítulo 2

ANÁLISE DE SISTEMAS ÓPTICOS DE DISTRIBUIÇÃO QUÂNTICA DE CHAVES COM PULSOS COERENTES FORTEMENTE ATENUADOS

Este capítulo discute a implementação prática de alguns dos principais sistemas de DQC com pulsos coerentes fracos. Os pulsos de fótons usados pelos sistemas deste capítulo são provenientes, na verdade, de pseudo-fontes de fótons isolados em que pulsos de luz coerentes com muitos fótons são fortemente atenuados de tal forma que a probabilidade do pulso conter nenhum ou um fóton é muito maior que ele conter dois ou mais.

2.1 Sistema de DQC Usando Interferômetro de Mach-Zehnder

O primeiro esquema interferométrico de DQC a ser analisado foi sugerido por Bennett, em 1992, e aperfeiçoado por Paul Townsend da British Telecom (BT) em 1995. O sistema consiste de um interferômetro de Mach-Zehnder, em que metade dele pertence à Alice (transmissor) e a outra metade a Bob (receptor). A configuração está mostrada na Figura 2.1.

No esquema, o pulso emitido pelo laser semiconductor no sistema óptico de Alice é fortemente atenuado pelo atenuador A antes de passar pelo acoplador óptico BS_1 , resultando em um pulso com número médio de fótons $\mu \ll 1$. Considerando que o pulso proveniente do laser apresenta distribuição de probabilidade do número de fótons Poissoniana, após ser atenuado, aproximadamente 90% dos pulsos conterão nenhum fóton (estado vácuo), enquanto 9% apresentarão um fóton e os restantes dos pulsos conterão dois ou mais fótons. Na seqüência, o pulso atenuado \perp entra no divisor de feixes BS_1 onde é dividido em outros

dois. Um deles percorre o braço longo onde é rotacionado de $+\pi/2$ pelo controlador de polarização e sofre um atraso de τ em relação ao outro. A outra metade percorre o braço mais curto e sofre modulação de fase ϕ_A quando passa pelo modulador de fase PM_A ($0, \pi/2, \pi$ ou $3\pi/2$, de acordo com o protocolo BB84). Dessa forma, os pulsos provenientes dos braços longo e curto são lançados no canal de fibra óptica, em tempos diferentes, através do acoplador óptico BS_2 . O objetivo de multiplexar, simultaneamente, os pulsos no tempo e na polarização é melhorar a visibilidade do interferômetro.

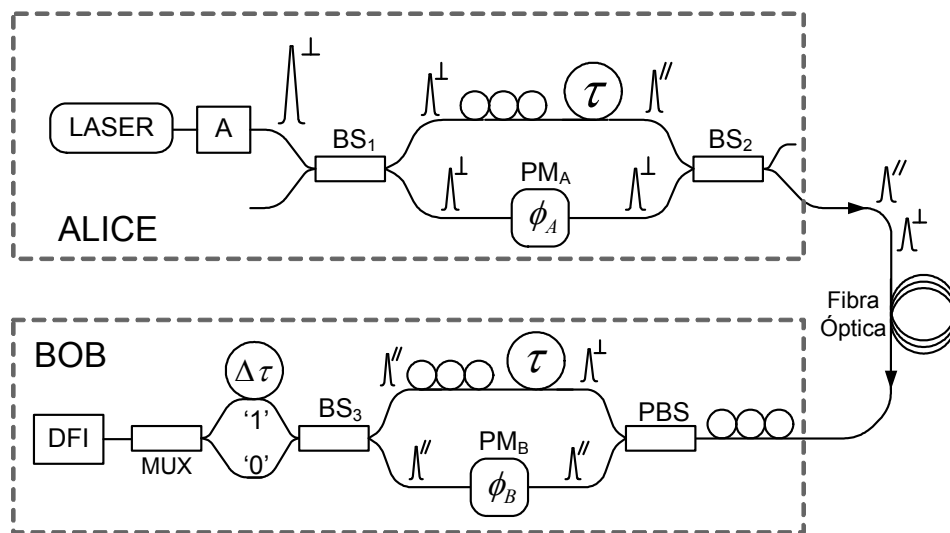


Figura 2.1: Implementação do sistema interferométrico de Mach-Zehnder para DQC. BS - acoplador óptico, PM - modulador de fase, DFI - detector de fótons isolados.

A função do controlador de polarização localizado logo na entrada do esquema de Alice é compensar efeitos da birrefringência da fibra na polarização dos pulsos. Os pulsos são então separados espacialmente pelo divisor por polarização (*PBS – Polarization Beam Splitter*). O pulso com polarização \perp que sofreu modulação de fase ϕ_A em Alice, percorre o braço longo onde sofre o mesmo atraso τ que o seu par sofreu em Alice e, além disso, tem sua polarização rotacionada de $\pi/2$, resultando em \parallel . Por outro lado, o pulso com polarização \parallel , que não sofreu modulação de fase por Alice, é enviado ao braço curto do interferômetro de Bob, onde sofre modulação de fase aleatória ϕ_B de 0 ou $\pi/2$ no modulador de fase PM_B . Assim, os pulsos chegam ao mesmo tempo e com a mesma polarização em BS_3 e sofrem interferência. Dependendo da diferença de fase dos pulsos modulados em

Alice e Bob, o pulso resultante emergirá em um dos braços de BS_3 (ou em ambos, quando o pulso possuir mais de um fóton e Alice e Bob escolherem bases diferentes). O braço identificado por '1' tem um laço de atraso $\Delta\tau$ que permite a separação temporal dos bits 1 e 0 no detector DFI , permitindo o uso de apenas um detector. O sistema de Bob registra os eventos como um par de dados, o qual representa o tempo decorrido desde o início da transmissão do bit por Alice e o intervalo de tempo que indica onde a detecção ocorreu dentro do período de emissão do pulso do laser [7]. Este período de tempo situa-se dentro de duas janelas de largura de 1ns do DFI, uma centrada em torno de 614ns para detecção de 1's e outra em 620ns para 0's, permitindo, assim, a diferenciação entre o que é informação e ruído.

O sistema experimental implementado pela BT [5,6] consistia, basicamente, dos seguintes elementos: enlace de fibra óptica de 30 km, diodo laser semiconductor operando 1330nm com taxa de emissão de 1MHz, produzindo pulsos de 30ps de duração e um detector de fótons isolados com fotodetector de avalanche de Germânio (Ge). Como dito anteriormente, as metades do pulso atenuado viajam no mesmo canal e a separação temporal entre eles é definida pela constante τ (5ns), definida por Alice. Deve ser levado em consideração que o tempo para que a variação das características do canal devido a efeitos ambientais seja maior que τ , e assim, os dois sofrem as mesmas perturbações impostas pelo canal. A necessidade de controladores de polarização no sistema é devido ao fato de que a interferência deve ser entre pulsos de mesma polarização. O polarizador na linha serve para restaurar a polarização degradada durante a propagação na fibra. Para o tipo de configuração adotado no sistema da BT, a taxa de transmissão alcançada foi de 1000bps, para um $QBER$ de 4% e com visibilidade de franja de 99%. Para um enlace de 10 km, a taxa de transmissão elevou-se para 20000bps com 1,5% de erro. Entretanto, para distâncias acima de 30 km, a taxa de transmissão é reduzida por um fator de 10. A eficiência deste sistema depende muito da eficiência de seu sistema de detecção de fótons, o qual contribui para o aumento da taxa de bits e redução da taxa de erro. O DFI usado apresentou eficiência de detecção de 20% para um resfriamento a 77K e com taxa de contagem de escuro em torno de 10^3 s^{-1} .

2.2 Sistema de DQC Plug&Play Usando Interferômetro de Michelson com Espelhos de Faraday

Este sistema foi desenvolvido pelo grupo de física da Universidade de Genebra (GAP-UG), em 1996. Ele é baseado em um interferômetro de Michelson com espelhos de Faraday, como mostra a Figura 2.2.

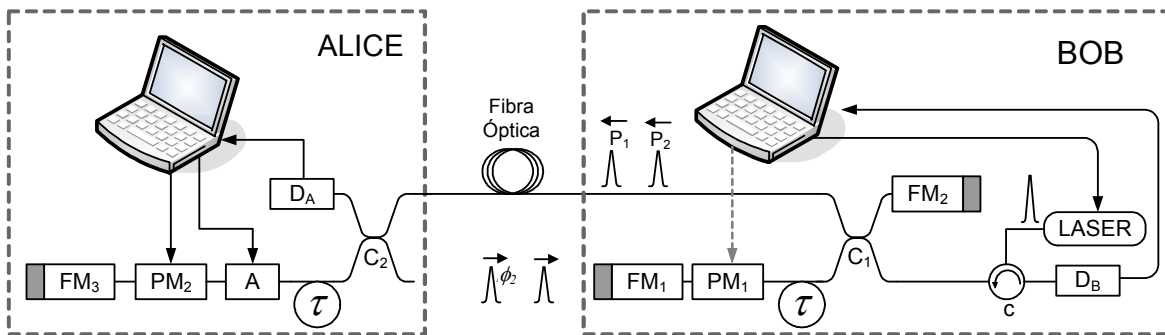


Figura 2.2: Interferômetro Plug&Play para DQC, protocolo B92, com espelhos de Faraday. FM - espelho de Faraday, $C_{1(2)}$ - acoplador, C – circulator.

O espelho de Faraday FM é um dispositivo óptico constituído de um espelho seguido de um rotacionador de Faraday de $\pi/4$. Conseqüentemente, o seu efeito resultante nos estados de polarização de pulsos incidentes é transformá-los em seus estados ortogonais na saída. Portanto, torna-se possível anular efeitos indesejáveis como a variação birrefringência, sendo dispensado o uso de controladores de polarização que são utilizados no sistema descrito na seção anterior. Além disso, este sistema não requer controle de comprimentos dos caminhos por onde os pulsos propagam, uma vez que estes seguem o mesmo caminho óptico, embora multiplexados no tempo [8]. Se os pulsos percorressem caminhos diferentes, os pulsos obteriam fases diferentes e isto causaria erro durante a troca da chave.

Bob começa a comunicação enviando para Alice um pulso de laser de curta duração, que passa pelo circulator C e chega ao acoplador balanceado C_1 onde é dividido em outros dois pulsos P_1 e P_2 . O primeiro segue diretamente para Alice, enquanto o segundo, P_2 , sofre três ações ainda em Bob. Primeiramente, ele sofre um atraso devido o percurso entre FM_1 e FM_2 . Depois, o seu estado de polarização é rotacionado de π rad ($\pi/2$ de FM_1 e $\pi/2$ de

FM₂). Por fim, sua intensidade é atenuada em relação a P_1 , devido às duas vezes que passa por C_1 . Nesta etapa, o modulador de fase PM₁ não atua em nenhum dos pulsos e os pulsos são enviados para Alice multiplexados no tempo.

Em Alice, os pulsos são divididos pelo acoplador C_2 e refletidos pelo espelho FM₃. O atenuador A é fixado em um determinado valor para que número médio de fótons em P_2 seja $\mu \approx 0,1$ fótons. Além disso, como P_1 chega primeiro ao aparato de Alice, metade dele aciona o modulador que irá modular P_2 em fase de acordo com o protocolo B92. Após isso, P_2 com modulação $\hat{\phi}_2$, P_1 e P_2 retornam a Bob. Ao retornar para Bob, metade de P_1 passa pelas mesmas ações sofridas por P_2 : um atraso de percurso entre FM₁ e FM₂; e seu estado de polarização é rotacionado de π rad, ficando equivalente ao de P_2 . A outra metade segue direto para o detector D_B que ativa o modulador de fase PM₁ com base em um mecanismo de temporização. Este modulador, por sua vez, baseado no protocolo B92, modula a outra metade do pulso P_1 citada anteriormente no momento em que ele é refletido por FM₁, dando-lhe uma fase $\hat{\phi}_1$. Sendo assim, P_1 e P_2 encontram-se temporalmente e espacialmente em C_1 , interferindo construtivamente se $\hat{\phi}_1 - \hat{\phi}_2 = 0$, ou destrutivamente, se $\hat{\phi}_1 - \hat{\phi}_2 = \pi$. Esta interferência é então detectada por D_B . Os deslocamentos de fase 0 e π correspondem aos bits 0 e 1 respectivamente [3,8,9]. Através deste sistema de temporização de pulsos, Bob diferencia os pulsos portadores de informação dos pulsos oscilantes entre os espelhos FM₁ - FM₂ ou FM₂-FM₃ em D_B .

O sistema experimental Plug&Play do GAP-UG [10] foi realizado sobre um enlace de fibra óptica comercial para 1330nm de 23km de distância, entre as cidades Nyon (Alice) e Genebra (Bob) na Suíça, com perdas de 8,6 dB. O laser usado foi um DFB da Fujitsu emitindo na janela de 1330nm, produzindo pulsos ópticos com largura de 300ps a uma taxa de emissão de 1kHz. O modulador de fase PM₁ de Bob é constituído de uma fibra envolvida ao redor de um modulador piezo elétrico de 10kHz, enquanto o de Alice, PM₂, é um guia de onda de Niobato de Lítio (LiNbO₃) que ser atuado em até 1GHz. Essa frequência tão alta é para garantir que apenas o pulso P_2 sofra modulação. A dependência de polarização deste tipo de modulador de fase foi eliminada pelas ações dos espelhos de Faraday. O enlace de atraso FM₁ - FM₂ tem 23m de comprimento que equivale a um intervalo de 250ns de separação entre os pulsos. O contador de fótons em Bob trata-se de

um fotodiodo de avalanche (FDA) de germânio resfriado em nitrogênio líquido a 77K, com eficiência de quântica de 10% e probabilidade de contagem de escuro de 7×10^{-6} . As dificuldades deste tipo de sistema estão relacionadas com a taxa de repetição do laser. A baixa taxa de repetição utilizada (1kHz) garante que não existirá mais que um pulso na fibra óptica por vez. Quando se aumenta a frequência, a taxa de erro de bit se eleva por causa do aparecimento de fótons refletidos e contagens pós-pulsos nos fotodetectores [11]. Altas taxas de transmissão são responsáveis também pelo espalhamento inverso de Rayleigh, que é resultante da natureza intrínseca bidirecional deste tipo de sistema interferométrico, pois os pulsos viajando para Alice e para Bob se cruzam. Estes pulsos retro-espalhados podem assim acompanhar um pulso propagando de volta para Bob e elevar a taxa de erro. O interferômetro apresentou excelente visibilidade de 99,84% e alta estabilidade, bem como baixas taxas de erro e de transmissão de bits como mostrado na Tabela 2.1[10].

μ - número médio de fótons por pulso	QBER (%)	Taxa de transmissão (bps)
0,2	$0,5 \pm 0,1$	0,9
0,1	$1,35 \pm 0,08$	0,5

Tabela 2.1: Resultados experimentais do sistema Plug&Play com interferômetro de Michelson usando espelhos de Faraday.

2.3 Sistema de DQC Plug&play Usando Interferômetro Mach-Zehnder com Protocolo BB84

O sistema de DQC analisado nessa seção também foi desenvolvido no GAP-UG, em 1998, e trata-se de uma modificação no sistema analisado na seção anterior. Seu diagrama esquemático está mostrado na Figura 2.3. Diferentemente do sistema da seção anterior, este é constituído de um interferômetro de Mach-Zehnder com um espelho de Faraday. Além disso, este sistema tem como fatores importantes a compensação dos efeitos de birrefringência e o auto-alinhamento. Vale ressaltar que todas as fibras e componentes ópticos de Bob mantêm a polarização dos pulsos no seu esquema de constante.

A transmissão é iniciada por Bob com o envio de um pulso de pequena largura através do circulador C e é, então, dividido em outros dois pulsos P_1 e P_2 pelo acoplador

balanceado C_1 . O pulso P_1 segue pelo braço curto do interferômetro e chega ao divisor de feixe de luz por polarização PBS . No caminho, sua polarização é rotacionada de $\pi/2$ pelo controlador de polarização localizado no braço curto. Já o pulso P_2 percorre o braço mais longo, sofre um atraso τ de 50ns em relação ao pulso P_1 , é também lançado ao canal, mas não sofre atuação do modulador de fase PM_1 .

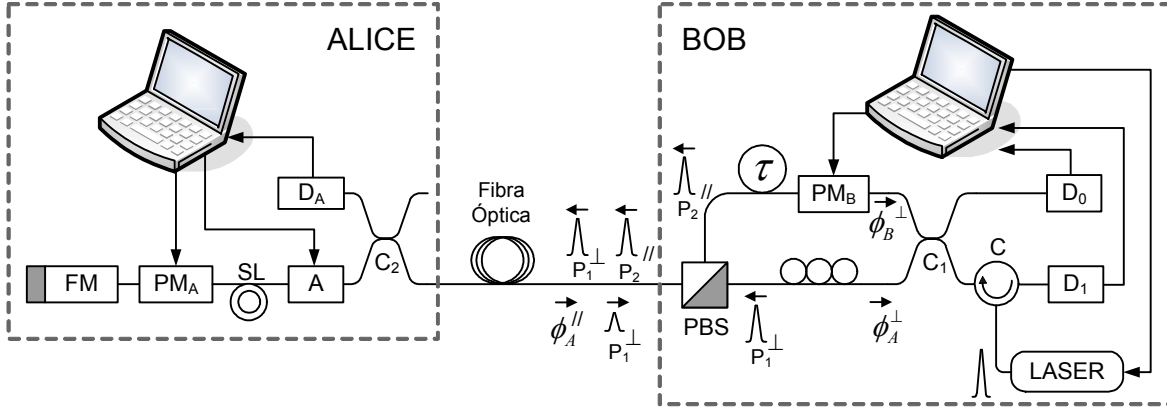


Figura 2.3: Diagrama esquemático do sistema interferométrico Plug&Play com protocolo BB84.

Portanto, os pulsos estão multiplexados no tempo. Ao chegar no aparato óptico de Alice, P_1 é dividido pelo acoplador 10/90, sendo que 10% do pulso fornecerá um sinal de sincronismo para ativação do modulador de fase que modulará a fase do pulso atrasado P_2 . O restante do pulso P_1 é refletido por FM ortogonalmente polarizado para Bob. P_2 é então modulado por PM_2 conforme o protocolo BB84 e refletido de volta para Bob com seu estado de polarização acrescido de $\pi/2$ e com fase $\widehat{\phi}_A$. Antes de serem lançados de volta para Bob, eles são atenuados pelo atenuador variável A de tal modo que o número médio de fótons por pulso seja de $\mu \approx 0,2$. Quando chegam em Bob, agora com polarizações invertidas em relação a que estavam no início, os pulsos invertem os caminhos por onde passaram. P_1 é refletido por PBS , percorre o braço longo, sofre o mesmo atraso de P_2 e é modulado por PM_B , obtendo fase $\widehat{\phi}_B$. O pulso P_2 é transmitido pelo PBS , e sofre rotação na polarização de $\pi/2$. Portanto, os dois pulsos alcançam o acoplador C_1 simultaneamente, com mesma polarização e interferem entre si. A diferença de fase $\widehat{\phi}_A - \widehat{\phi}_B$ determina se o fóton será detectado por D_0 (detecção de bits 0) ou por D_1 (detecção de bits 1).

O protótipo é simples de ser usado. Basta apenas conectar as extremidades dos aparatos de Alice e Bob a um enlace de fibra óptica. Os DFIs usam fotodiodos de avalanche resfriados com elemento *Peltier*, circuito de extinção no modo engatilhado com largura de pulso de gatilho de 2,5ns. Os pulsos aplicados aos moduladores de fase PM_A e PM_B para modulação dos pulsos P_1 e P_2 tem largura aproximada de 50ns. As contagens de escuro foram medidas no início da operação, tendo com resultado uma probabilidade de escuro $p_{esc} \approx 10^{-5}$ por gatilho. Mesmo que o sistema não necessite de alinhamento óptico, os gatilhos de modulação de fase e detecção devem ser aplicados no tempo correto. O armazenador de pulsos (*SL*) consiste de uma fibra de aproximadamente 10km que acomoda 480 pulsos ópticos de 260ps a 5MHz. O detector D_A de Alice é bem mais simples, consistindo apenas de um fotodiodo PIN com amplificador rápido para detecção de pulsos multifótons enviados por Bob. O sinal elétrico gerado pela detecção em D_A é usado para informar a Alice que ela prepare seu modulador de fase PM_A para o pulso que está chegando. Além disso, ele tem a função de monitorar possíveis tentativas de espionagem.

Além das vantagens citadas anteriormente, esta versão minora os problemas relacionados às altas taxas de repetição do laser: o espalhamento inverso de Rayleigh e os efeitos dos pós-pulsos nos detectores. Os efeitos do primeiro problema forma resolvidos com a introdução do armazenador de pulsos *SL* no aparato de Alice. Com sua capacidade de até 480 pulsos, ela receberá um novo trem de pulsos a cada vez que o trem de pulsos anterior tenha retornado para Bob. Dessa forma, o espalhamento de Rayleigh se concentrará no lado de Alice, mas a sua intensidade será reduzida pelo atenuador variável *A*. Experimentos mostraram que, com isso, as falsas contagens resultantes de fótons espalhados inversamente são três vezes menores que as contagens de escuros, sendo desprezadas. Em relação aos efeitos de pós-pulso, foram solucionados com uso de fotodiodos de avalanche de InGaAs/InP.

O ponto mais sensível deste sistema é sua sensibilidade à estratégia de ataque conhecida como cavalo de Tróia [1]. Este ataque consiste no envio de pulsos por Eva, através do canal quântico para Alice ou Bob, e na análise dos mesmos após serem refletidos pelo espelho de Faraday. Deste modo, Eva pode obter informações sobre o laser, os detectores e os moduladores de fase. Para prevenir tal ataque, o atenuador localizado em

Alice reduz a quantidade de luz que se propaga pelo sistema. Além disso, também monitora a intensidade dos pulsos incidentes por meio do detector D_A [1,11].

Foram feitos testes experimentais em diferentes enlaces de fibra óptica comerciais já instalados. A fim de facilitar a operação, durante os testes foi sempre usada a mesma seqüência de bits aleatória, em cada enlace. Dessa forma, Bob realizou peneiragem e cálculo da taxa de erro sem comunicação com Alice. A Tabela 1.2 mostra os resultados da transmissão da chave com $\mu \approx 0,2$ [12].

Enlace	Comprimento (km)	Perdas (dB)	Visibilidade (%)
Geneve-Nyon ⁽¹⁾	22,0	4,8	99,70 ± 0,03
Geneve-Nyon ⁽²⁾	22,6	7,4	99,81 ± 0,03
Nyon-Lausanne ⁽²⁾	37,8	10,6	99,63 ± 0,05
Geneve-Nyon ⁽¹⁾ A	67,1	14,4	99,62 ± 0,06
Geneve-Nyon ⁽¹⁾ B	67,1	14,3	99,66 ± 0,05
Ste. Croix ⁽³⁾	8,7	3,8	99,70 ± 0,01
Ste. Croix ⁽³⁾	23,7	7,2	99,71 ± 0,01

Tabela 2.2: Medidas de visibilidade do sistema Plug&Play.

Enlace	Comprimento (km)	K (kbit)	R_{Bruta} (kHz)	QBER (%)	$R_{Liquida}$ (kHz)
Geneve-Nyon ⁽¹⁾	22,0	27,9	2,06	2,0 ± 0,1	1,51
Geneve-Nyon ⁽²⁾	22,6	27,5	2,02	2,1 ± 0,1	1,39
Nyon-Lausanne ⁽²⁾	37,8	25,1	0,50	3,9 ± 0,2	0,26
Geneve-Nyon ⁽¹⁾ A	67,1	12,9	0,15	6,1 ± 0,4	0,044
Geneve-Nyon ⁽¹⁾ B	67,1	12,9	0,16	5,6 ± 0,3	0,051
Ste. Croix ⁽³⁾	8,7	63,8	6,29	3,0 ± 0,1	4,34
Ste. Croix ⁽³⁾	23,7	117,6	2,32	3,0 ± 0,1	1,57

Tabela 2.3: Resultados do sistema Plug&Play para diferentes enlaces de fibra óptica. K é o comprimento inicial da chave.

2.4 Sistema de DQC com Modulação de Fase Relativa entre Bandas Laterais

Nesta seção é descrito um sistema óptico que usa interferência construtiva ou destrutiva entre bandas laterais de um sinal óptico que são obtidas por moduladores de fase

ou amplitude, em Alice e Bob, alimentados por um sinal de RF com baixo índice de modulação, para implementar um sistema de DQC [13-18]. O aparato óptico fundamental é mostrado na Figura 2.4 [18].

Alice utiliza como fonte de luz um diodo laser operando numa frequência central ω_0 . Além disso, ela possui um oscilador de fase travada (PLO) operando na frequência Ω , um modulador óptico de fase ou amplitude e um modulador de fase de RF que imprime ao sinal de RF de Alice a fase Φ_1 .

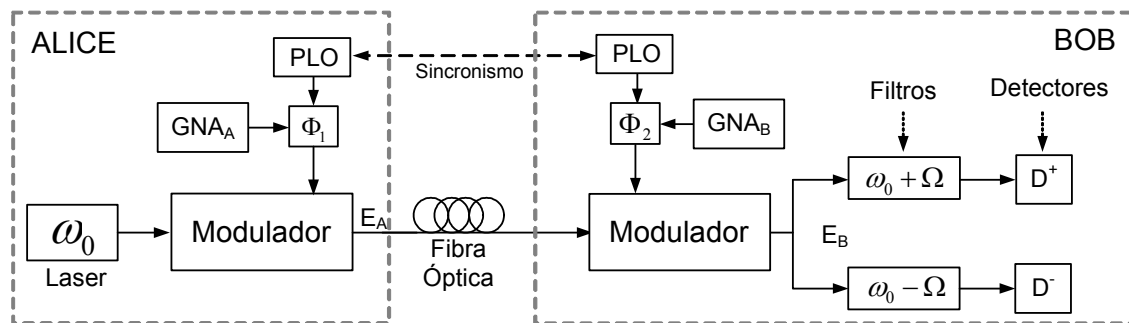


Figura 2.4: Aparato óptico usado para modulação de fase relativa entre bandas laterais. GNA – gerador de números aleatórios, PLO – oscilador de fase travada.

Do outro lado, Bob também usa um modulador óptico semelhante ao de Alice e o seu gerador de RF opera com a mesma frequência Ω e com sincronismo de fase em relação ao de Alice. Já o seu modulador de fase de RF imprime ao sinal de RF gerado por ele a fase Φ_2 . Por fim, Bob usa detectores de fótons isolados com filtros ópticos para separar as bandas laterais. Os blocos GNA_A e GNA_B que alimentam os moduladores de fase de Alice e Bob, respectivamente, geram a seqüência aleatória de bits usada por cada um deles conforme o protocolo a ser implementado (BB84 ou B92). O resultado da modulação do sinal óptico no lado de Alice, além da portadora centrada em ω_0 , é o surgimento de duas bandas laterais, uma centrada em $\omega_0 + \Omega$ e outra em $\omega_0 - \Omega$ com fase Φ_1 . No lado de Bob, o sinal óptico proveniente de Alice sofre nova modulação, sendo geradas mais duas bandas laterais em $\omega_0 \pm \Omega$ com fase Φ_2 . Supondo índice de modulação muito menor que a unidade, os segundos harmônicos gerados a partir das bandas laterais provenientes de Alice são desprezados. Assim, dependendo da diferença de fase $\Phi_1 - \Phi_2$, ocorrerá interferência construtiva ou destrutiva. Para que isso ocorra com melhor visibilidade possível, é essencial

que os geradores de Alice e Bob operem exatamente na mesma frequência Ω e que eles estejam em fase. Para tal propósito, é necessário o uso de um enlace de sincronismo. Será detalhado na seção 2.4.4 a implementação de um sistema que utiliza sincronismo WDM para contornar esse problema [17]. Nas seções 2.4.1-2.4.3 são mostrados os principais resultados das possíveis combinações: PM-PM, AM-AM e AM-PM [18].

2.4.1 Modulação PM – PM

Considere que Alice utiliza como fonte de luz um diodo laser operando numa frequência central ω_0 e cuja expressão do campo elétrico é dada por [17]

$$E_1 = E_0 e^{j\omega_0 t}, \quad (2.1)$$

em que E_0 é a amplitude do campo. Ao passar pelo modulador óptico de fase de Alice, o campo E_A na saída deste é [18]

$$E_A = E_0 e^{j\omega_0 t} e^{j[m \cos(\Omega t + \Phi_1)]}, \quad (2.2)$$

em que Ω é a frequência do sinal de RF e Φ_1 é o valor de fase escolhido por Alice e m é o índice de modulação. Supondo m muito menor que a unidade, (2.2) resulta em [18]

$$E_A = E_0 e^{j\omega_0 t} \left\{ 1 + j \frac{m}{2} \left[e^{j(\Omega t + \Phi_1)} + e^{-j(\Omega t + \Phi_1)} \right] \right\}. \quad (2.3)$$

Após percorrer um enlace de fibra com comprimento L , o sinal na entrada do modulador óptico de fase de Bob é [18]

$$E_F = E_0 \left\{ e^{j(\beta_0 L + \omega_0 t)} + j \frac{m}{2} \left[e^{j(\beta_+ L + (\omega_0 + \Omega)t + \Phi_1)} + e^{-j(-\beta_- L - (\omega_0 - \Omega)t + \Phi_1)} \right] \right\}, \quad (2.4)$$

em que β_0 , β_+ e β_- são as constantes de propagação para cada componente de frequência de E_F . Desprezando efeitos de dispersão cromática, β_{\pm} são dadas por:

$$\beta_{\pm} = \frac{n}{c}(\omega_0 \pm \Omega). \quad (2.5)$$

Por fim, o campo após o modulador de fase de Bob, o campo resultante é [18]

$$E_B = E_F e^{j[m \cos(\Omega t + \Phi_2)]}. \quad (2.6)$$

Sendo assim, considerando que o índice de modulação em Bob também é muito menor que a unidade, (2.6) resulta em

$$\begin{aligned} E_B = E_0 e^{j\omega_0 t} + E_0 j \frac{m}{2} \left\{ e^{j\left[\frac{n}{c}\Omega L + (\omega_0 + \Omega)t + \Phi_1\right]} + e^{-j\left[\frac{n}{c}\Omega L - (\omega_0 - \Omega)t + \Phi_1\right]} \right\} + \\ + E_0 j \frac{m}{2} \left\{ e^{j[(\omega_0 + \Omega)t + \Phi_2]} + e^{-j[-(\omega_0 - \Omega)t + \Phi_2]} \right\} = E_B^{\omega_0} + E_B^{\omega_0 + \Omega} + E_B^{\omega_0 - \Omega}. \end{aligned} \quad (2.7)$$

Vale destacar que, em (2.7), os termos resultantes multiplicados por m^2 foram desprezados, pois são muito pequenos. Sendo assim, com base em (2.7), as intensidades de cada banda lateral após o modulador de Bob, que são definidas por

$$I_B^{\omega_0 \pm \Omega} = E_B^{\omega_0 \pm \Omega} \times (E_B^{\omega_0 \pm \Omega})^*, \quad (2.8)$$

são idênticas e dadas por [18]

$$I_B^{\omega_0 \pm \Omega} = \frac{E_0^2 m^2}{2} \left[1 + \cos\left(\frac{n}{c}\Omega L + \Delta\Phi\right) \right], \quad (2.8)$$

em que $\Delta\Phi = \Phi_1 - \Phi_2$. Portanto, (2.8) mostra que a probabilidade do fóton ser encontrado será igual para as duas bandas. A Figura 2.5 ilustra o resultado do espectro de frequência para os possíveis valores de $\Delta\Phi$.

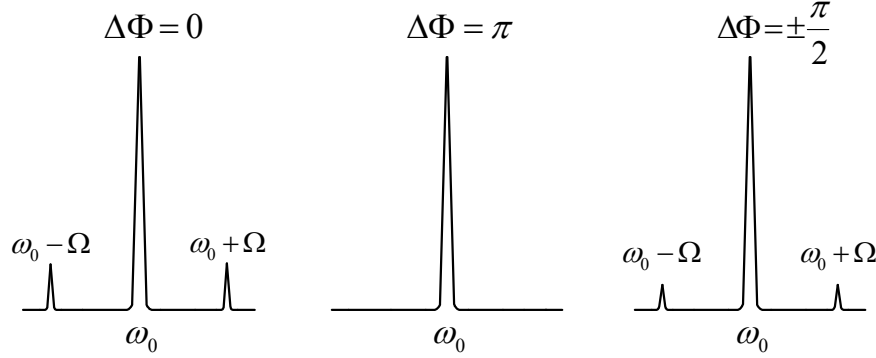


Figura 2.5: Espectro de frequência do pulso óptico na saída do modulador de Bob.

Como pode ser observado na Figura 2.5, a intensidade das bandas laterais é máxima quando $\Delta\Phi = 0$ e mínima quando $\Delta\Phi = \pi$. No caso $\Delta\Phi = \pm\pi/2$, as bandas apresentam intensidades intermediárias. Considerando agora a mesma análise, mas agora no regime quântico, $\Delta\Phi = 0$ significa que existirá, com probabilidade máxima, um fóton em uma das raias laterais, $\Delta\Phi = \pi$ significa que não existirá um fóton em nenhuma delas e $\Delta\Phi = \pm\pi/2$ significa que existirá ou não um fóton em uma delas, mas com probabilidade intermediária. Com base no exposto, é possível a aplicação do protocolo B92 conforme a Tabela 2.4 [18].

Na implementação do protocolo B92, Bob registra todos os instantes em que houve contagem em qualquer um dos seus detectores para as bandas $\omega_0 + \Omega$ e $\omega_0 - \Omega$. No final da transmissão, ele informa à Alice esses instantes e em todos os outros os valores são descartados.

Bit	Alice	Bob	$\omega_0 + \Omega$	$\omega_0 - \Omega$
0	0	0	SIM	SIM
	0	π	NÃO	NÃO
1	π	0	NÃO	NÃO
	π	π	SIM	SIM

Tabela 2.4: Implementação do protocolo B92 para sistema PM-PM.

Portanto, a menos de contagens de escuro nos detectores e eventuais erros de transmissão, os dois sabem qual o valor que cada um inferiu. Por fim, para que a segurança seja garantida para os casos de ataques individuais, a taxa de erro do sistema não deve ultrapassar 15%. Para uma última análise, o sistema não suporta a versão original do BB84. Isso seria possível se a interferência resultante se comportasse de forma complementar.

2.4.2 Modulação AM – AM

Nesta seção é mostrado o caso em que Alice e Bob usam moduladores ópticos Mach-Zehnder de amplitude. Em verdade, este sistema se comporta de forma semelhante ao apresentado na seção anterior em que é utilizada a modulação PM-PM [18].

Na análise a ser feita, Alice tem o mesmo equipamento mostrado na Figura 2.4 com exceção do modulador que é de amplitude. Novamente, o pulso proveniente do laser, que é dado por (2.1), é modulado com um sinal de RF com frequência Ω e a informação a ser transmitida é sobreposta a esse sinal usando desvios de fase Φ_1 . Além disso, o modulador é polarizado com uma tensão DC que gera um desvio de fase Ψ_1 em um dos braços do MZ conforme Figura 2.6.

Após o modulador de Alice, a expressão do campo na sua saída é dada por [18]

$$E_A = \frac{E_0 e^{j\omega_0 t}}{\sqrt{2}} \left[1 + e^{j(\Psi_1 + m \cos(\Omega t + \Phi_1))} \right]. \quad (2.9)$$

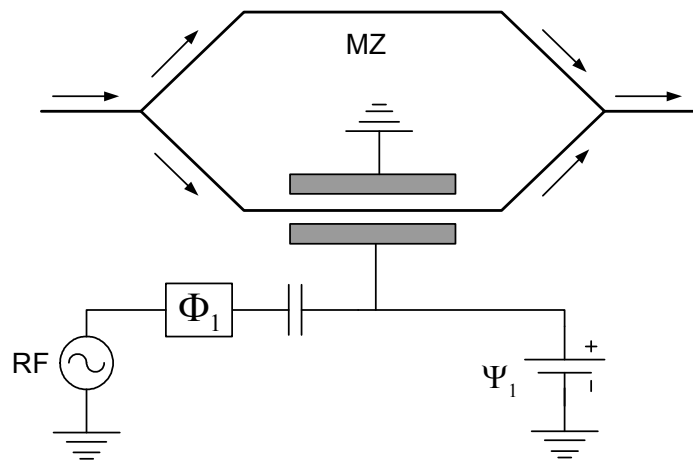


Figura 2.6: Diagrama de um modulador de Mach-Zehnder.

Considerando novamente o índice de modulação m muito menor que a unidade, (2.9) fica:

$$E_A = \frac{E_0 e^{j\omega_0 t}}{\sqrt{2}} \left\{ 1 + e^{j\Psi_1} \left[1 + j \frac{m}{2} \left(e^{j(\Omega t + \Phi_1)} + e^{-j(\Omega t + \Phi_1)} \right) \right] \right\}. \quad (2.10)$$

Portanto, a intensidade $I_A = E_A E_A^*$ é

$$I_A = \frac{E_0^2}{2} \left[1 + \cos \Psi_1 - m \sin \Psi_1 \cos(\Omega t + \Phi_1) \right]. \quad (2.11)$$

Com base em (2.11), se $\Psi_1 = (\pi/2$ ou $3\pi/2)$ a modulação é máxima e, assim, a intensidade das bandas laterais também são máximas. Se $\Psi_1 = 0$, apenas a portadora não modulada deixará o modulador, enquanto que se $\Psi_1 = \pi$, não sairá luz do modulador. Como é desejada modulação máxima, é considerado $\Psi_1 = 3\pi/2$. Assim, chega-se na expressão geral para qualquer modulador de amplitude:

$$E_A = \frac{E_0 e^{j\omega_0 t}}{\sqrt{2}} \sqrt{1 + m \cos(\Omega t + \Phi_1)} \quad (2.12)$$

Novamente, considerando m muito pequeno, (2.12) se reduz a

$$E_A = \frac{E_0 e^{j\omega_0 t}}{\sqrt{2}} \left\{ 1 + \frac{m}{4} \left[e^{j(\Omega t + \Phi_1)} + e^{-j(\Omega t + \Phi_1)} \right] \right\}. \quad (2.13)$$

Propagando o campo (2.13) através de uma fibra óptica de comprimento L , o sinal E_F na entrada do modulador de Bob é [18]

$$E_F = \frac{E_0}{\sqrt{2}} \left\{ e^{j(\beta_0 L + \omega_0 t)} + \frac{m}{4} \left[e^{j(\beta_+ L + (\omega_0 + \Omega)t + \Phi_1)} + e^{-j(-\beta_- L - (\omega_0 - \Omega)t + \Phi_1)} \right] \right\}. \quad (2.14)$$

Desprezando novamente a dispersão cromática, o pulso após o modulador de Bob, e considerando também $\Psi_2=3\pi/2$, é dado por [18]

$$E_B = \frac{E_F}{\sqrt{2}} \left\{ 1 + \frac{m}{4} \left[e^{j(\Omega t + \Phi_2)} + e^{-j(\Omega t + \Phi_2)} \right] \right\}. \quad (2.15)$$

Com base em (2.15), as intensidades de cada banda lateral após o modulador de Bob, que são definidas em (2.8), são idênticas e dadas por [18]

$$I_B^{\omega_0 \pm \Omega} = \frac{E_0^2 m^2}{32} \left[1 + \cos \left(\frac{n}{c} \Omega L + \Delta \Phi \right) \right]. \quad (2.16)$$

Portanto, os sistemas que usam PM-PM e AM-AM se comportam de forma semelhante, podendo também ser implementado o B92 neste último. Além disso, ambos os sistemas podem executar o protocolo BB84 modificado, sendo usado apenas um DFI centrado em apenas uma das bandas laterais. Esse protocolo, apesar de funcionar com o mesmo princípio do BB84 original, apresenta uma séria desvantagem, dado que a taxa de bits cai pela metade, pois agora apenas 25% das escolhas de bases estarão corretas contra 50% do BB84 original [18].

2.4.3 Modulação AM – PM (PM – AM)

O sistema apresentado nesta seção usa a combinação de moduladores de fase e amplitude, ou vice-versa, por Alice e Bob. É demonstrado em [18] que as intensidades das bandas laterais se comportam complementarmente, possibilitando a implementação do BB84 original. Na análise realizada aqui, é aproveitado todo o equacionamento feito nas duas seções anteriores para os PM-PM e AM-AM. Considerando que Alice tem um modulador de amplitude e Bob um de fase, o campo na saída deste último é [18]

$$\begin{aligned}
 E_B = E_0 e^{j\omega_0 t} + E_0 \frac{m_1}{4} \left\{ e^{j\left[\frac{n}{c}\Omega L + (\omega_0 + \Omega)t + \Phi_1\right]} + e^{-j\left[\frac{n}{c}\Omega L - (\omega_0 - \Omega)t + \Phi_1\right]} \right\} + \\
 + j \frac{E_0 m_2}{4} \left\{ e^{j[(\omega_0 + \Omega)t + \Phi_2]} + e^{-j[-(\omega_0 - \Omega)t + \Phi_2]} \right\}, \quad (2.17)
 \end{aligned}$$

sendo que m_1 e m_2 são os índices de modulação para os moduladores de Alice e Bob respectivamente. O procedimento para o cálculo das intensidades é semelhante ao que foi feito anteriormente. Assim, as intensidades são [18]

$$I_B^{\omega_0 + \Omega} = \frac{E_0^2}{8} \left[\frac{m_1^2}{4} + m_2^2 + m_1 m_2 \sin\left(\frac{n}{c}\Omega L + (\Phi_1 - \Phi_2)\right) \right], \quad (2.18)$$

$$I_B^{\omega_0 - \Omega} = \frac{E_0^2}{8} \left[\frac{m_1^2}{4} + m_2^2 - m_1 m_2 \sin\left(\frac{n}{c}\Omega L + (\Phi_1 - \Phi_2)\right) \right]. \quad (2.19)$$

Como podemos observar de (2.18) e (2.19), as duas bandas se comportam complementarmente. A Tabela 2.5 mostra a os possíveis resultados para implementação do protocolo BB84 clássico e a Figura 2.7 mostra os espectro de freqüência do pulso na saída no modulador de Bob para os possíveis valores de $\Phi_1 - \Phi_2$ [18].

		Bit	Alice	Bob	$\omega_0 + \Omega$	$\omega_0 - \Omega$
Base ₁ (0 e π)	0	0	0	0	SIM	NÃO
		0	$\pi/2$	$\pi/2$?	?
	1	π	0	0	NÃO	SIM
		π	$\pi/2$	$\pi/2$?	?
		Bit	Alice	Bob	$\omega_0 + \Omega$	$\omega_0 - \Omega$
Base ₂ ($\pi/2$ e $-\pi/2$)	0	$\pi/2$	0	0	?	?
		$\pi/2$	$\pi/2$	$\pi/2$	SIM	NÃO
	1	$-\pi/2$	0	0	?	?
		$-\pi/2$	$\pi/2$	$\pi/2$	NÃO	SIM

Tabela 2.5: Implementação do protocolo BB84 para sistema AM-PM.

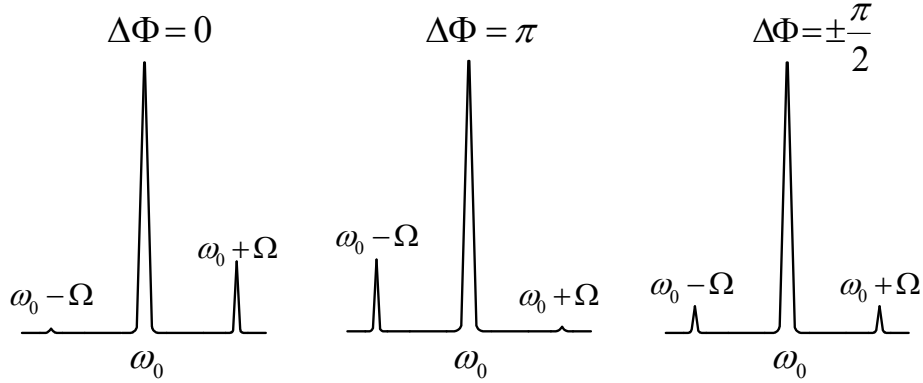


Figura 2.7: Espectro de frequência do pulso óptico na saída do modulador de Bob para o caso AM-PM.

2.4.4 Implementação de Sistema de DQC com BB84 modificado Usando Modulação de Fase Relativa entre Bandas Laterais com Sincronismo WDM

A principal dificuldade nas implementações dos esquemas apresentados nas seções 2.4.1-2.4.3 são suas sensibilidade a variações das características da fibra tais como comprimento, atenuação e efeitos não-lineares que afetam o sinal recebido por Bob. Em particular, a pequena diferença entre os comprimentos de onda do pico central e das bandas laterais torna o sistema sensível a variações do caminho de transmissão, influenciando diretamente na visibilidade V do interferômetro. Sendo assim, em [17] é proposto um esquema capaz de compensar os efeitos causados pelas variações de caminho e os efeitos de dispersão cromática que possam prejudicar sincronismo do sistema como um todo. Isso foi realizado graças a um sinal de referência que é enviado em um comprimento de onda diferente do usado pelo canal quântico no mesmo enlace de fibra óptica. A implementação do experimento está detalhada na Figura 2.8.

Os dois sinais, o quântico e o de sincronismo, são multiplexados pelo *MUX WDM* e lançados simultaneamente no canal. No lado de Bob, eles são separados pelo *DEMUX WDM*, e o sinal de sincronismo, que traz a referência de fase, é usado tanto para alimentar o MZI_2 como para controlar a detecção e a demodulação do pulso óptico no aparato óptico de Bob. No esquema da Figura 2.8, os pulsos de luz são gerados em Alice por um diodo laser de 2mW operando em 1547,43nm.

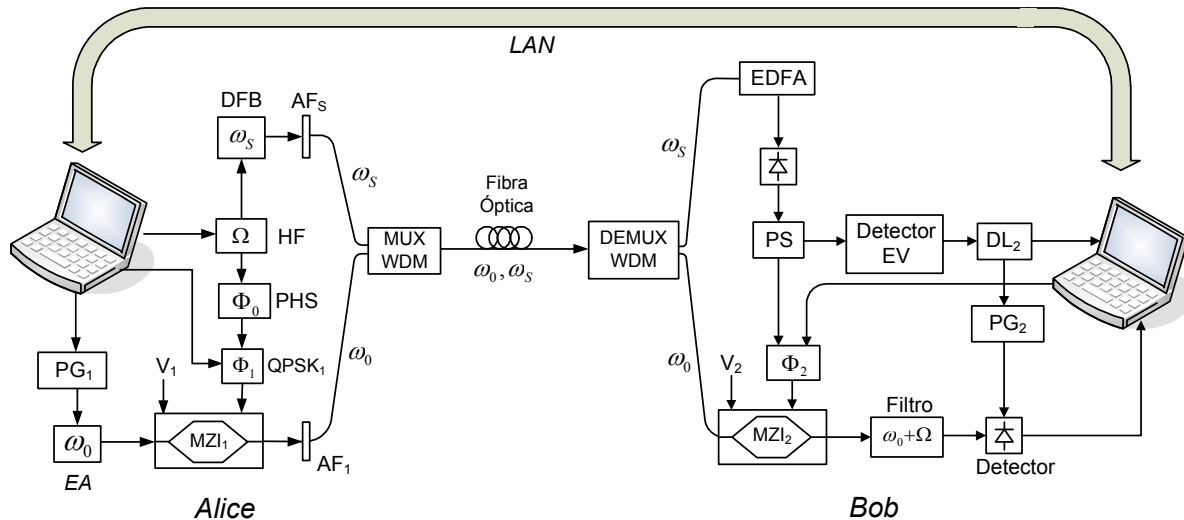


Figura 2.8: Esquema experimental usado no sistema de DQC com sincronismo WDM. PG - gerador de pulsos, HF – Gerador de microondas, PHS - deslocador de fase, QPSK - modulador de fase, $AF_{s(1)}$ – atenuadores ópticos, DL - linha de atraso.

Cada pulso óptico tem aproximadamente 8ns e são emitidos a uma taxa de 1MHz, graças ao gerador de pulsos PG_1 que é controlado pelo computador de Alice. Um sinal de 2GHz com baixo índice de modulação é gerado por um sintetizador de microondas (HF) que modula o interferômetro de Mach-Zender MZI_1 . O deslocador de fase (PHS) ajusta a fase deste sinal para Φ_0 . Além disso, o computador controla o modulador de fase $QPSK_1$, que introduz a fase aleatória Φ_1 que pode assumir qualquer valor no conjunto de valores de fases do protocolo BB84 que são $\{0, \pi/2, \pi, 3\pi/2\}$. Antes de o pulso ser lançado no canal, ele é atenuado pelo atenuador ajustável AF_1 , que reduz a energia de cada pulso para um número médio de fótons de aproximadamente $\mu=0,2$ para ambas as bandas laterais. Já o sinal de sincronismo é gerado por um diodo laser de modulação direta (DFB) operando em 1552,43 nm. O sinal de 2GHz é modulado em amplitude com o mesmo sinal de 1MHz gerado por PG_1 para alimentar o DFB . Esse pulso de sincronismo deve ter um nível de energia tal que possa ser detectado corretamente pelo receptor e que evite *crosstalk* com o sinal enviado pelo canal quântico. Ele é filtrado e atenuado para uma potência 600nW. Finalmente, é então lançado no canal de fibra óptica juntamente com o sinal quântico através do multiplexador óptico WDM (MUX).

No lado de Bob, tanto o sinal quântico quanto o sinal de sincronismo nas frequências ω_0 e ω_s são separados pelo demultiplexador óptico WDM (*DEMUX*). O sinal de sincronismo é então utilizado para extrair o sinal que gera a frequência de 2GHz e a fase de referência que são usadas para alimentar MZI_2 com um deslocamento de fase inicial Φ_2 . Esse deslocamento de fase é controlado por computador através de um modulador de fase QPSK, $QPSK_2$. Pode-se observar que o sistema utiliza apenas um detector. Assim, a fase Φ_2 é escolhida entre os valores $\{0, \pi/2, \pi, 3\pi/2\}$. Essa modificação permite a detecção de bits 0 e 1 pelo mesmo detector. O sinal de sincronismo é primeiramente amplificado por um EDFA para que possa ser detectado corretamente. Depois, o sinal elétrico resultante é dividido e filtrado em dois diferentes caminhos para obter um sinal na frequência de 2GHz e outro de 1MHz. Esse sinal de 1MHz dispara o MZI_2 e as janelas de detecção. Além disso, para garantir o sincronismo, o tempo de atuação do gatilho deve ser bem estabelecido. Sendo assim, é introduzida a linha de atraso DL_2 que é calibrada para ser sincronizada com os pulsos de luz quânticos. Foi usado o fotodiodo de avalanche de InGaAs/InP Epitaxx EPM239 operando no modo engatilhado, com larguras de pulsos de gatilho de aproximadamente 10ns e amplitude 4,8V. A tensão reversa é de 50V, sendo a tensão de ruptura de 53V. Nestas condições a taxa de contagens de escuro por gatilho e a eficiência quântica foram, respectivamente, 8×10^{-6} e 10%. Uma LAN é usada como canal público de comunicação para realizar o processo de reconciliação do protocolo BB84.

A taxa de erro do sistema, considerando que apenas um detector é usado, é aproximadamente [17]

$$QBER = \frac{\frac{1-V}{4} p_{\text{exp}}^{\text{signal}} + \frac{1}{2} P_d}{P_d + \frac{p_{\text{exp}}^{\text{signal}}}{2}} \quad (2.20)$$

$$p_{\text{exp}}^{\text{signal}} = 1 - \exp(-\eta\mu\eta_T) \quad (2.21)$$

em que η é a eficiência do detector, η_T representa todas as perdas em função da distância incluindo aquelas devido à fibra e P_d é a probabilidade de contagem de escuro. Os experimentos foram realizados com enlaces de fibra óptica de 20 km e 40 km. A

visibilidade medida foi de 98% e as perdas no detector foram de 9,8 dB. A Tabela 2.6 traz um comparativo entre o sistema apresentado nesta seção e alguns sistemas já realizados [17].

Grupo de Pesquisa	λ (nm)	Distância (km)	μ	F (kHz)	R_{Bruta} (Hz)	QBER (%)
B.T.	1300	30	0,2	1000	260	4
Los Alamos	1300	48	0,63	100	20	9,3
Genève	1550	67	0,2	5000	160	5,6
Nec Lab.	1550	100	0,2	500	5,5	10
Toshiba	1550	101	0,1	500	5,5	10
G.T.L.	1550	40	0,2	1000	400	3

Tabela 2.6: Comparação entre os sistemas já realizados e, em negrito, está o descrito nesta seção.

2.5 Implementação de um Sistema de DQC Polarimétrico de Alta Taxa de Transmissão.

Em todos os sistemas apresentados anteriormente pode-se facilmente constatar a baixa taxa de transmissão de bits úteis alcançada. Como mostra a equação (1.4), isto se deve ao baixo número médio de fótons do pulso utilizado, às perdas nos dispositivos ópticos e à baixa eficiência dos detectores. Não é possível aumentar o número médio de fótons dos pulsos utilizados sem comprometer a segurança, nem diminuir as perdas de fibras ópticas que já se encontram próximas do limite teórico. Portanto, a seleção do fotodiodo de avalanche é crucial para o desempenho do sistema de DQC. Os FDAs podem ser feitos de silício (Si) para a faixa de 300–1100nm, de germânio (Ge) para a faixa de 800–1600nm ou de arseneto de gálio índio (InGaAs) para faixa de 900–1700nm. O comportamento dos três tipos diferentes de FDAs é mostrado na Figura 2.9. Esta mostra a potência de ruído equivalente (NEP - *noise equivalent power*) que é definida pela potência óptica requerida para medir uma relação sinal-ruído unitária, com intervalo de integração de um segundo, e é dado por:

$$NEP = \frac{hv}{\eta} \cdot \sqrt{2R_{esc}}, \quad (2.22)$$

onde h é a constante de Planck, ν é a frequência dos fótons e R_{esc} é taxa de contagem de escuro (*darkcount rate*).

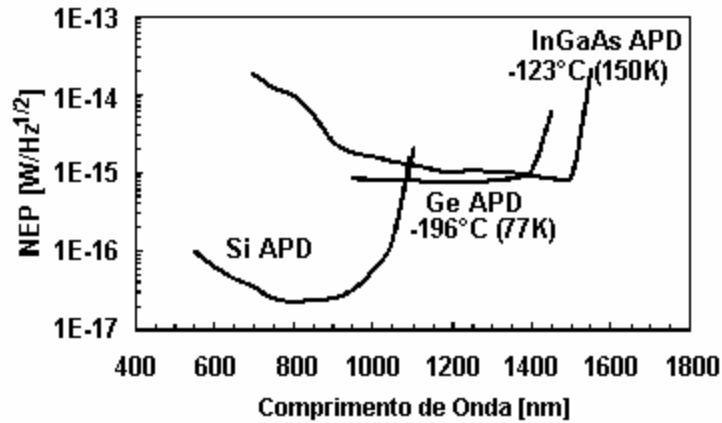


Figura 2.9: *NEP* versus comprimento de onda para FADs de Si, Ge e de InGaAs.

O FDA de Si chega a apresentar eficiência quântica η superior a 70%, tempo jitter inferior a 400 ps e probabilidade de contagem de escuro na ordem de 10^{-8} em uma temperatura de -20 °C (253K). Eles encontram aplicações em DQC no espaço livre e em sistema de DQC de curto alcance devido às perdas na fibra serem da ordem de 2 dB/km em torno de 850nm. Os FADs de Ge e InGaAs, por operarem nas duas janelas de telecomunicações, 1,30 μ m e 1,55 μ m, onde as perdas na fibra são bem inferiores, 0,35dB/km e 0,2dB/km, respectivamente, são usados em transmissão de longa distância (dezenas de quilômetros). Desprezando o $QBER_{opt}$ e usando os dados da Tabela 2.7, a Figura 2.10 caracteriza o comportamento dos FADs para curtas distâncias ($L < 25$ km). Observa-se que o FDA de Si é excelente para distâncias inferiores a 21km. Por outro lado, para transmissão em longas distâncias, a melhor opção é o FDA de InGaAs/InP.

FDA	Perdas na Fibra (dB/km)	Probabilidade de Contagem de Escuro (p_{esc})	Eficiência Quântica de Detecção η
Si (800 nm)	2	10^{-8}	0,5
Ge (1300 nm)	0,35	$21 \cdot 10^{-6}$	0,2
InGaAs (1550 nm)	0,2	10^{-5}	0,1

Tabela 2.7: Parâmetros típicos de FADs de Si, Ge e de InGaAs disponíveis comercialmente.

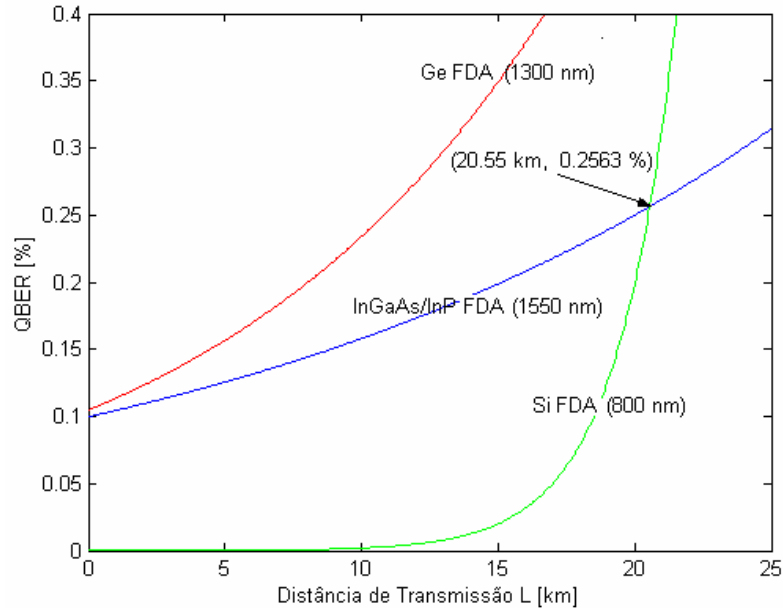


Figura 2.10: Comportamento teórico de FODs de Si, Ge e de InGaAs em distâncias curtas para $\mu=0,1$ $\nu=10\text{MHz}$, e dados da Tabela 2.7.

Portanto, se o objetivo é construir um sistema de DQC, usando fótons isolados, de alta velocidade, o mesmo deve ser utilizado em curtas distâncias e utilizar FODs de silício. Um sistema de DQC de alta velocidade, com as características citadas, utilizando polarização da luz e executando o protocolo B92 foi proposto em [19-21]. O sistema implementado em [19,20] é o mostrado na Figura 2.11.

Observando o esquema da Figura 2.11, pode-se imediatamente reconhecer o sistema da Figura 1.5. Alice usa dois lasers do tipo VCEL (vertical-cavity surface emitting laser) operando em 850nm, um para o bit 0 e o outro para o bit 1. Além disso, Alice possui também um laser DFB operando em 1300nm. Este sinal, contendo aproximadamente $1,5 \cdot 10^8$ fótons por pulso, é usado para sincronismo, sendo detectado em Bob por um detector com fotodiodo de Ge. Devido à existência de dois comprimentos de onda diferentes, acopladores WDM são usados tanto em Alice quanto em Bob. Após os testes, realizados, para uma taxa de alimentação dos lasers de 1 GHz a 2 GHz e distância de 6,55 km, o QBER medido foi de 7% e a taxa de transmissão de bits úteis, isto é, após correção de erros e amplificação de privacidade, foi de 20kbit/s.

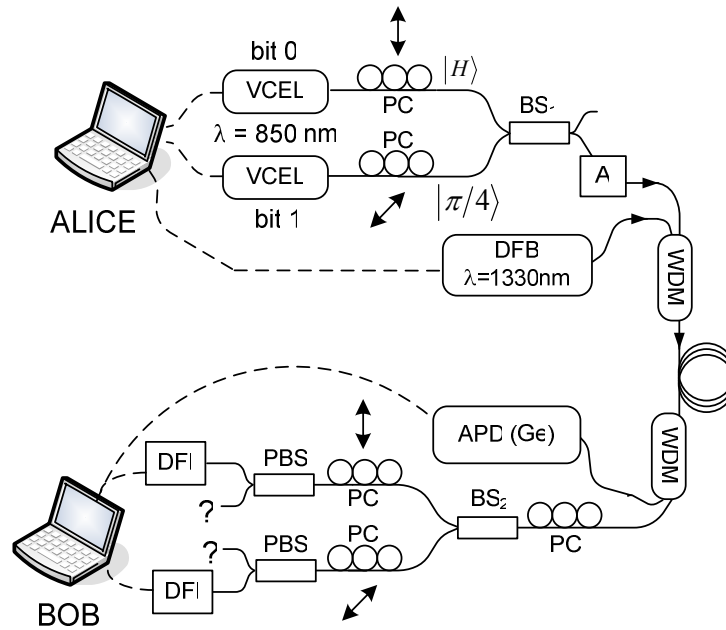


Figura 2.11: Esquema experimental usado na implementação do protocolo B92 de alta velocidade.

2.6 Distribuição Quântica de Chaves com Interferômetro de Sagnac

A primeira proposta de DQC usando o interferômetro de Sagnac, chamada DQC tipo circular, foi feita na referência [22]. O esquema óptico proposto é o mostrado na Figura 2.12.

Inicialmente Bob envia um pulso óptico de muitos fótons. Este pulso é dividido no acoplador C em dois outros, sendo que um segue para Alice no sentido horário, P_H , enquanto que o outro segue para Alice no sentido anti-horário P_{AH} . O pulso P_H chega primeiro em Alice, pois o pulso P_{AH} passa primeiro pela linha de atraso. Ao chegar em Alice, o pulso P_H sofre uma atenuação em A, passa por PC_A e PM_A e segue de volta a Bob. Chegando em Bob, P_H passa pela linha de atraso, passa por PC_B , sofre uma modulação de fase em PM_B e, por fim, chega ao acoplador C. O pulso P_{AH} passa por PM_B , PC_B , linha de atraso e segue pelo canal óptico para Alice. Em Alice, P_{AH} sofre modulação de fase em PM_A , depois passa por PC_A , é atenuado em A e segue para o acoplador C de Bob. Ambos os pulsos chegam em C ao mesmo tempo e sofrem interferência. Dependendo da diferença das fases aplicadas por Alice em P_{AH} e por Bob em P_H , o pulso será guiado para o detector de fótons isolados D_0 ou D_1 .

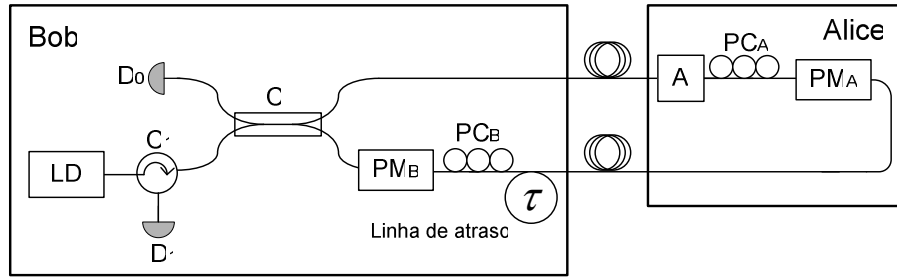


Figura 2.12: Distribuição quântica de chaves tipo circular.

Uma vez que ambos os pulsos percorrem o mesmo caminho físico, flutuações de diferenças de fase são automaticamente compensadas. Os controladores de polarização PC_A e PC_B fazem o controle da polarização para minimizar a taxa de erro. O valor de atenuação do atenuador A é tal que quando o pulso P_{AH} deixar Alice ele tenha o número médio de fótons igual 0,1. O sistema da Figura 1.11 foi experimentalmente implementado e os resultados reportados na referência [22] são: taxa de transmissão de bits úteis 1200bps, visibilidade 89,4% e taxa de erro 5,4%. O experimento foi realizado na janela de 850nm, utilizando detectores de fótons isolados de silício, taxa de modulação do laser de 100kHz, distância entre Alice e Bob de 200m e linha de atraso de 800m.

A segunda proposta de DQC usando o interferômetro de Sagnac foi feita na referência [23]. O esquema óptico proposto é o mostrado na Figura 2.13. O sistema da Figura 2.13 trabalha de forma similar ao da Figura 2.12, entretanto, no esquema da Figura 2.13, os moduladores de fase utilizados são acusto-ópticos e, por isso, são insensíveis à variação da polarização. Isto torna o sistema mais simples pois faz desnecessário o rigoroso sistema de controle da polarização requerido pelo sistema da Figura 2.12 que utiliza moduladores de fase de Niobato de Lítio ($LiNbO_3$).

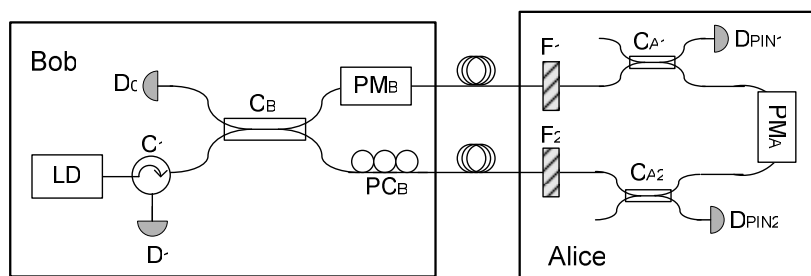


Figura 2.13: Distribuição quântica de chaves com interferômetro Sagnac.

A segunda diferença é a presença dos filtros ópticos F_1 e F_2 , acopladores ópticos C_{A1} e C_{A2} e os detectores clássicos D_{PIN1} e D_{PIN2} . A presença destes componentes é para evitar ataques do tipo Cavalo de Tróia. Neste ataque, a espiã envia um pulso óptico forte para Alice e analisa os pulsos transmitidos e refletidos a fim de tirar informações sobre qual valor de fase Alice utilizou. Assim, os filtros ópticos evitam que Eva utilize pulsos de grande largura espectral para analisar a variação do espectro do pulso refletido ou transmitido e os detectores clássicos D_{PIN1} e D_{PIN2} percebem se Eva enviou um pulso forte através da detecção de parte do mesmo desviada pelo acoplador C_{A1} ou C_{A2} , dependendo do sentido que Eva enviou o pulso, horário ou anti-horário.

2.7 Segurança de Sistemas de DQC Utilizando Estados Coerentes Fracos

Foi provado que os protocolos BB84 [24,25] e B92 [26,27] quando implementados com fontes reais de fótons isolados são perfeitamente seguros. Entretanto, uma vez que tais fontes não estão ainda plenamente disponíveis, a solução que permite a implementação de protocolos de DQC é a utilização de fontes de estados coerentes fortemente atenuados, como as utilizados nos esquemas das Seções 2.1-2.5. A utilização de estados coerentes atenuados permite à espiã Eva obter informação sem ser descoberta. Isto ocorre devido à existência de pulsos multifótons. Na análise de segurança é comum dar à espiã total poder tecnológico. Assim, é normal assumir que a espiã pode realizar medição não demolidora [28] do número de fótons dos pulsos enviados por Alice, possui memória quântica e pode fornecer um caminho mais curto e/ou fibra de menor perda entre ela e Bob. O ataque por separação de fótons (PNS - photon number splitting attack) é como segue: Eva intercepta os pulsos enviados por Alice e mede de forma não demolidora o número de fótons do mesmo. Se o pulso contiver um fóton, a espiã barra o fóton, não deixando passar nada para Bob. Se o pulso contiver mais que um fóton, a espiã retira um fóton do pulso e encaminha o(s) demais para Bob por um canal óptico de perda menor, o que compensa os fótons por ela barrados. Se Bob não for capaz de medir o número de fótons dos pulsos que recebe para reconstruir a estatística Poissoniana dos pulsos enviados por Alice, Eva não será descoberta e obterá completa informação da chave, pois, uma vez que ela contém cópias perfeitas dos fótons recebidos por Bob armazenadas em sua memória quântica, quando Alice e Bob

avisarem quais bases foram usadas, Eva medirá seus fótons nas bases corretas e obterá completa informação sobre a chave. Para o protocolo B92 a situação é ainda mais dramática, pois Eva não precisará ter nem memória quântica nem medição quântica não demolidora do número de fótons. Basta Eva utilizar o mesmo aparato de Bob. Toda vez que ela obtiver uma medição conclusiva, Eva envia um pulso óptico para Bob com o mesmo qubit. Se Eva não obtiver um resultado conclusivo, ela nada envia para Bob. Um componente crucial neste ataque são as perdas do enlace entre Alice e Bob, pois quando Eva barra um pulso óptico, Alice e Bob desconfiarão que o fóton foi consumido pelas perdas. Assim, Alice e Bob podem garantir a segurança do sistema de DQC que usam se ambos estiverem próximos o suficiente (ou seja, pouca perda no canal óptico entre eles), de forma a proibir Eva de barrar todos os pulsos com apenas um fóton. Sendo forçada a barrar apenas uma fração dos pulsos, Eva não terá informação completa. Portanto, o ataque por separação de fótons limita a distância entre Alice e Bob. Eva pode ainda optar por, ao invés de barrar os pulsos que contém apenas um fóton, fazer um ataque por máquina de clonagem neles. Nestes casos, a probabilidade sucesso de Eva é de aproximadamente 0,86%. Assim, nenhuma das implementações apresentadas nas Seções 2.1-2.5 é resistente ao ataque por separação de fótons, entretanto, implementações de sistemas de DQC resistentes ao PNS foram propostas nas referências [29-31].

Capítulo 3

SISTEMA DE DISTRIBUIÇÃO QUÂNTICA DE CHAVES COM MODULAÇÃO DE FASE RELATIVA ENTRE BANDAS LATERAIS USANDO MULTIPORTADORAS

Uma evolução natural do sistema apresentado na Seção 2.4, que usa modulação de fase relativa entre bandas laterais de frequência, é a possibilidade de serem usadas mais de uma portadora para transmissão da informação por canais quânticos paralelos [32], utilizando moduladores de fase em Alice e amplitude em Bob, ou vice-versa. Baseado nesta idéia, no presente capítulo é apresentado um esquema que emprega duas portadoras de radiofrequência no sistema AM-PM descrito na Seção 2.4.3 para execução de dois protocolos BB84 que operam paralelamente.

3.1 Sistema de Distribuição Quântica de Chaves com Modulação de Fase Relativa entre Bandas Laterais Usando Multiportadoras.

O sistema a ser analisado é apresentado na Figura 3.1 e é semelhante àquele em que Alice possui um modulador de amplitude usando um interferômetro de Mach-Zehnder e Bob possui um modulador de fase, como descrito na Seção 2.4.3.

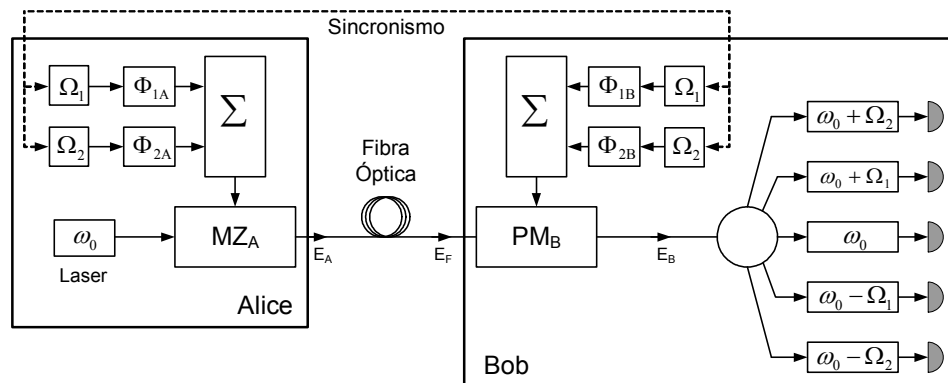


Figura 3.1: Diagrama esquemático para o sistema de DQC com multiportadoras.

Inicialmente, o campo na saída do modulador de amplitude de Alice é dado por

$$E_A = \frac{E_0 e^{j\omega_0 t}}{2} \left\{ 1 + e^{j\Psi_1} e^{j[m_1 \cos(\Omega_1 t + \Phi_{1A}) + m_2 \cos(\Omega_2 t + \Phi_{2A})]} \right\}, \quad (3.1)$$

em que $m_{1(2)}$ e $\Omega_{1(2)}$ são os índices de modulação e as frequências usadas para as portadoras nos canais quânticos 1 e 2, respectivamente. Além disso, Φ_{1A} e Φ_{2A} são as fases das radiofrequências Ω_1 e Ω_2 que portarão a informação enviada por Alice, conforme o protocolo de DQC a ser implementado. Considerando $m_{1(2)}$ muito menores que a unidade, a equação (3.1) pode ser aproximada por:

$$E_A = \frac{E_0 e^{j\omega_0 t}}{2} \left\{ 1 + e^{j\Psi_1} \left[1 + jm_1 \cos(\Omega_1 t + \Phi_{1A}) \right] \left[1 + jm_2 \cos(\Omega_2 t + \Phi_{2A}) \right] \right\}. \quad (3.2)$$

Logo, a intensidade do campo definido em (3.2) pode ser calculada e é dada por

$$I_A = \frac{E_0^2}{2} \left\{ 1 + \cos \Psi_1 - m_1 \sin \Psi_1 \cos(\Omega_1 t + \Phi_{1A}) - m_2 \sin \Psi_1 \cos(\Omega_2 t + \Phi_{2A}) \right\}. \quad (3.3)$$

Sendo assim, para que ocorra modulação máxima como descrito na Seção 2.4.2, façamos $\Psi_1 = 3\pi/2$. Substituindo este valor de Ψ_1 em (3.2) ou (3.3), pode-se encontrar que

$$\begin{aligned} E_A &= \frac{E_0}{\sqrt{2}} \sqrt{1 + m_1 \cos(\Omega_1 t + \Phi_{1A}) + m_2 \cos(\Omega_2 t + \Phi_{2A})} e^{j\omega_0 t} \approx \\ &\approx \frac{E_0}{\sqrt{2}} e^{j\omega_0 t} \left\{ 1 + \frac{m_1}{2} \cos(\Omega_1 t + \Phi_{1A}) + \frac{m_2}{2} \cos(\Omega_2 t + \Phi_{2A}) \right\}. \end{aligned} \quad (3.4)$$

Em (3.4) a fase global foi desconsiderada. Após percorrer um enlace de fibra L , o sinal na entrada do modulador de fase de Bob é

$$E_F = \frac{E_0}{\sqrt{2}} \left\{ e^{j(\beta_0 L + \omega_0 t)} + \frac{m_1}{4} \left[e^{j(\beta_1^+ L + (\omega_0 + \Omega_1)t + \Phi_{1,A})} + e^{-j(-\beta_1^- L - (\omega_0 - \Omega_1)t + \Phi_{1,A})} \right] \right\} + \frac{E_0}{\sqrt{2}} \frac{m_2}{4} \left[e^{j(\beta_2^+ L + (\omega_0 + \Omega_2)t + \Phi_{2,A})} + e^{-j(-\beta_2^- L - (\omega_0 - \Omega_2)t + \Phi_{2,A})} \right], \quad (3.5)$$

em que β_0 , $\beta_{1(2)}^+$ e $\beta_{1(2)}^-$ são as constantes de propagação em cada componente de frequência de E_F . Desprezando efeitos de dispersão cromática, $\beta_{1(2)}^\pm$ são dadas por:

$$\beta_{1(2)}^\pm = \frac{n}{c} (\omega_0 \pm \Omega_{1(2)}). \quad (3.6)$$

Por fim, desprezando em (3.5) o termo $e^{j\beta_0 L}$, pois representa uma fase global, (3.5) fica

$$E_F = \frac{E_0}{\sqrt{2}} \left\{ e^{j\omega_0 t} + \frac{m_1}{4} \left[e^{j\left(\frac{n}{c}\Omega_1 L + (\omega_0 + \Omega_1)t + \Phi_{1,A}\right)} + e^{-j\left(\frac{n}{c}\Omega_1 L - (\omega_0 - \Omega_1)t + \Phi_{1,A}\right)} \right] + \frac{m_2}{4} \left[e^{j\left(\frac{n}{c}\Omega_2 L + (\omega_0 + \Omega_2)t + \Phi_{2,A}\right)} + e^{-j\left(\frac{n}{c}\Omega_2 L - (\omega_0 - \Omega_2)t + \Phi_{2,A}\right)} \right] \right\}. \quad (3.7)$$

O campo após o modulador de fase óptico de Bob é, então, dado por

$$E_B = E_F e^{j[m_3 \cos(\Omega_1 t + \Phi_{1,B}) + m_4 \cos(\Omega_2 t + \Phi_{2,B})]}. \quad (3.8)$$

Em (3.8) $m_{3(4)}$ são os índices de modulação usados no modulador de fase de Bob para os canais quânticos 1 e 2, respectivamente. Além disso, Φ_{1B} e Φ_{2B} são as fases das radiofrequências Ω_1 e Ω_2 escolhidas por Bob, conforme o protocolo de DQC. Novamente, considerando $m_{3(4)}$ muito menores que a unidade, (3.8) pode ser aproximada por

$$\begin{aligned}
 E_B &= E_F \left[1 + jm_3 \cos(\Omega_1 t + \Phi_{1B}) \right] \left[1 + jm_4 \cos(\Omega_2 t + \Phi_{2B}) \right] \\
 &= E_F \left[\begin{array}{c} 1 + jm_3 \cos(\Omega_1 t + \Phi_{1B}) + jm_4 \cos(\Omega_2 t + \Phi_{2B}) - \\ - m_3 m_4 \cos(\Omega_1 t + \Phi_{1B}) \cos(\Omega_2 t + \Phi_{2B}) \end{array} \right]. \quad (3.9)
 \end{aligned}$$

Substituindo (3.7) em (3.9) obtemos

$$\begin{aligned}
 E_B &= \frac{E_0}{\sqrt{2}} \left\{ \begin{array}{l} e^{j\omega_0 t} + \frac{m_1}{4} \left[e^{j\left(\frac{n}{c}\Omega_1 L + (\omega_0 + \Omega_1)t + \Phi_{1A}\right)} + e^{-j\left(\frac{n}{c}\Omega_1 L - (\omega_0 - \Omega_1)t + \Phi_{1A}\right)} \right] + \\ + \frac{m_2}{4} \left[e^{j\left(\frac{n}{c}\Omega_2 L + (\omega_0 + \Omega_2)t + \Phi_{2A}\right)} + e^{-j\left(\frac{n}{c}\Omega_2 L - (\omega_0 - \Omega_2)t + \Phi_{2A}\right)} \right] \end{array} \right\} \times \\
 &\quad \left\{ \begin{array}{c} 1 + jm_3 \cos(\Omega_1 t + \Phi_{1B}) + jm_4 \cos(\Omega_2 t + \Phi_{2B}) - \\ - m_3 m_4 \cos(\Omega_1 t + \Phi_{1B}) \cos(\Omega_2 t + \Phi_{2B}) \end{array} \right\}. \quad (3.10)
 \end{aligned}$$

Finalmente, as intensidades das bandas laterais para cada frequência de modulação $\Omega_{1(2)}$ podem ser calculadas de (3.10). Após simples, mas tediosos cálculos, temos

$$I_B^{(\omega_0 \pm \Omega_1)} = \frac{E_0^2}{8} \left[\frac{m_1^2}{4} + m_3^2 \pm m_1 m_3 \sin\left(\frac{n}{c}\Omega_1 L + \Delta\Phi_1\right) \right] e \quad (3.11)$$

$$I_B^{(\omega_0 \pm \Omega_2)} = \frac{E_0^2}{8} \left[\frac{m_2^2}{4} + m_4^2 \pm m_2 m_4 \sin\left(\frac{n}{c}\Omega_2 L + \Delta\Phi_2\right) \right], \quad (3.12)$$

em que $\Delta\Phi_1 = \Phi_{1A} - \Phi_{1B}$ e $\Delta\Phi_2 = \Phi_{2A} - \Phi_{2B}$. Com base em (3.11) e (3.12), pode-se inferir que as bandas laterais de cada canal quântico $\Omega_{1(2)}$ interferem independentemente. Além disso, fazendo $(n/c)\Omega_1 L = \pi/2$, $(n/c)\Omega_2 L = 3\pi/2$, $m_1 = 2m_3$ e $m_2 = 2m_4$ as equações (3.11) e (3.12) ficam da forma

$$I_B^{(\omega_0 + \Omega_1)} = \frac{E_0^2 m_1^2}{16} \cos^2\left(\frac{\Phi_{1A} - \Phi_{1B}}{2}\right) \quad (3.13)$$

$$I_B^{(\omega_0 - \Omega_1)} = \frac{E_0^2 m_1^2}{16} \text{sen}^2 \left(\frac{\Phi_{1A} - \Phi_{1B}}{2} \right) \quad (3.14)$$

$$I_B^{(\omega_0 + \Omega_2)} = \frac{E_0^2 m_2^2}{16} \text{sen}^2 \left(\frac{\Phi_{2A} - \Phi_{2B}}{2} \right) \quad (3.15)$$

$$I_B^{(\omega_0 - \Omega_2)} = \frac{E_0^2 m_2^2}{16} \text{cos}^2 \left(\frac{\Phi_{2A} - \Phi_{2B}}{2} \right) \quad (3.16)$$

Analisando as equações (3.13) e (3.14), elas são similares às equações (1.1) e (1.2) e, como tais, permitem a execução do protocolo BB84. O mesmo ocorre com as equações (3.15) e (3.16). Portanto, o sistema da Figura 3.1 permite a implementação em paralelo de dois protocolos BB84, o que implica, na prática, na possibilidade de dobrar a taxa de transmissão de bits úteis.

Capítulo 4

RESULTADOS EXPERIMENTAIS DA IMPLEMENTAÇÃO DO PROTOCOLO DE DISTRIBUIÇÃO QUÂNTICA DE CHAVES B92

Neste capítulo é discutida a implementação experimental de um sistema óptico executando o protocolo de DQC B92 com estados de polarização da luz e os resultados experimentais obtidos. O esquema construído é o mais simples e barato que pode ser feito, portanto, sua implementação é meramente didática. Na Seção 4.1 é feita uma rápida abordagem sobre detectores de fótons isolados e são mostrados os resultados experimentais da caracterização dos que foram usados na implementação do sistema proposto. Na Seção 4.2 são mostrados os resultados experimentais da implementação do protocolo B92.

4.1 Detectores de Fótons Isolados – DFI

Detectores de fótons isolados são dispositivos cruciais em tecnologia da informação quântica. Basicamente, dado que chegou um fóton, o DFI deve fornecer um pulso de saída TTL. O principal elemento do DFI é fotodiodo de avalanche (FDA). Quando um fóton único incide na janela de um FDA que está corretamente polarizado, este pode gerar, por processo de avalanche, um pulso de tensão detectável através de um resistor. Tal pulso é amplificado por um amplificador operacional rápido e formatado por lógica digital, resultando em pulso TTL na saída do detector. Os principais parâmetros que devem ser determinados nos testes iniciais de um DFI são: a eficiência quântica, η , que representa a probabilidade de um fóton gerar uma contagem, e a probabilidade de contagem de escuro, P_D , que representa a probabilidade de haver avalanche sem que um fóton tenha chegado ao detector. Ambos dependem da tensão reversa aplicada aos terminais do FDA, V_{FDA} , e de

sua temperatura T . Quanto maior (menor) for o valor de V_{APD} ou T , maior (menor) serão os valores de η e P_D .

Uma característica importante de um FDA é sua tensão de ruptura V_B . Se V_{APD} é menor que V_B , uma avalanche não pode ocorrer e, portanto, um fóton não pode ser detectado. Uma vez que uma avalanche foi disparada, ela deve ser extinta para não danificar o FDA. Existem três modos básicos de extinção: passiva, ativa e engatilhada. O modo passivo é o mais simples de ser realizado, mas tem altas taxas de erros, pois uma contagem de escuro pode acontecer a qualquer instante. O modo ativo possibilita taxas rápidas, pois a avalanche é extinta rapidamente. No experimento de DQC apresentado neste capítulo foi utilizado o modo engatilhado, portanto, é ele que é discutido em mais detalhes.

No modo engatilhado, o FDA está na maior parte do tempo polarizado reversamente abaixo de V_B . Um gerador de pulsos gera (idealmente) pulsos quadrados com amplitude V_G que são usados para aumentar V_{FDA} acima de V_B durante curtas janelas de tempo, T_w . Durante T_w , $V_{FDA} = V + V_G > V_B$ e um fóton pode ser detectado. A diferença $V_{FDA} - V_B$ é chamada tensão de excesso, V_e . Quanto maior (menor) for V_e , maior (menor) é η e P_D . Na Figura 4.1 é mostrado o circuito básico para detecção de fótons isolados com extinção engatilha e a seqüência de pulsos de gatilho.

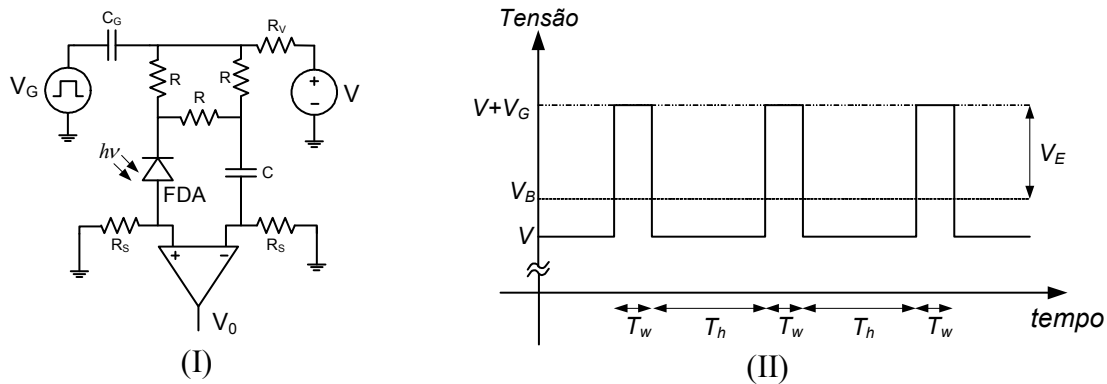


Figura 4.1: FDA sob modo de extinção engatilhado (I) e trem de pulsos de gatilhos (II).

O intervalo de tempo T_w em que V_{FDA} é maior que V_B é também um outro parâmetro importante para o desempenho do detector. Quanto menor T_w , menor o número de contagens de escuro. Como o FDA estará apto a detectar fótons apenas em determinados intervalos de tempo, o pulso de gatilho e o pulso de luz devem chegar ao mesmo tempo no

FDA. Além disso, após uma avalanche ter sido extinta, o FDA necessita de um intervalo de recuperação. Portanto, existe um tempo de desuso em que o dispositivo fica desabilitado a sofrer uma nova avalanche. Se esse tempo não for respeitado, as contagens de escuro aumentam devido aos efeitos de contagem de pós-pulso (*afterpulsing*). Obviamente, tal tempo é um limitador da taxa de transmissão em que o sistema de DQC pode operar. Baseado nisto, devem ser então determinados os parâmetros de operação η , P_D , T_w e T_h .

O ponto ótimo de operação do FDA é o ponto que minimiza o *NEP* (*Noise Equivalent Power*), que é uma figura de mérito que estabelece a melhor relação entre sinal ruído do FDA. O *NEP* é dado por [1]

$$NEP = \left(\frac{h\nu}{\eta} \right) \sqrt{P_D T_w}, \quad (4.1)$$

em que $h\nu$ é a energia do fóton. Para encontrar o ponto ótimo de operação, dado que T_w e T_h foram escolhidos, sendo T_w o menor valor possível (valores típicos entre 2ns e 10ns) e T_h o grande suficiente para tornar o efeito de pós-pulso desprezível, deve-se determinar a tensão de excesso V_e e a temperatura do FDA, e calcular o *NEP* para cada possível valor de ambos. Nos experimentos realizados, o pulso de gatilho usado pode ser visto na Fig. 4.2. O esquema usado para caracterização do FDA é mostrado na Figura 4.3.

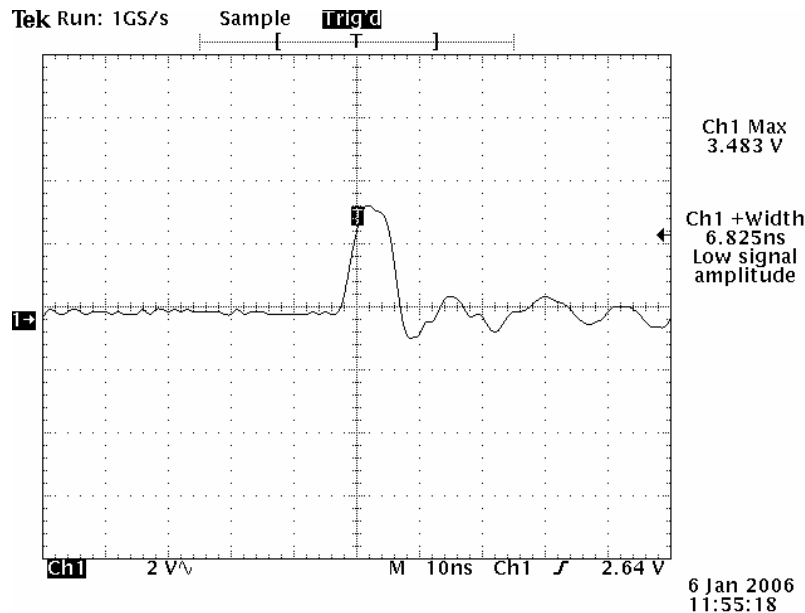


Figura 4.2: Pulso de gatilho experimental.

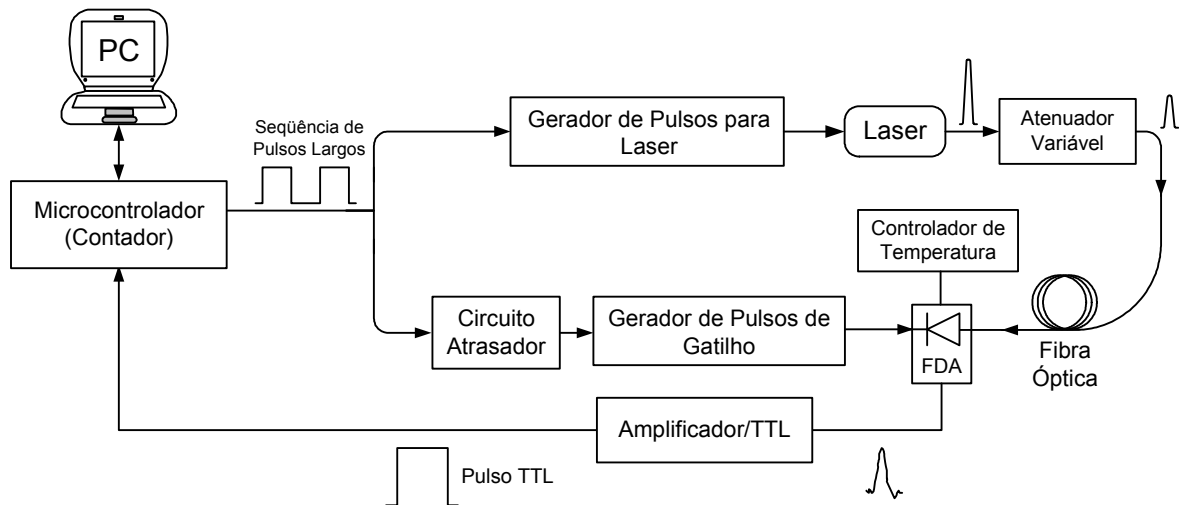


Figura 4.3: Esquema usado na caracterização do FFA.

O gerador de pulsos foi desenvolvido pelo LATIQ na UFC. Ele envia pulso de gatilho para o FFA e um outro pulso mais fino ao diodo laser CQF915/108 operando em 1550,9nm. Este último pulso está mostrado na Figura 4.4.

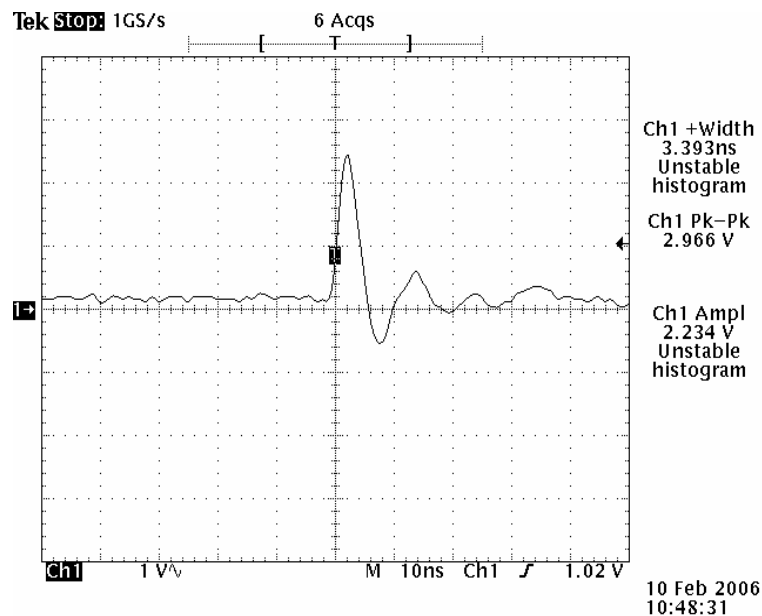


Figura 4.4: Pulso elétrico experimental que modula o laser.

O circuito de atraso também foi desenvolvido pelo LATIQ. Ele controla a separação entre o pulso de gatilho e o pulso que modula o laser de tal forma que a chegada do fóton

coincida com a chegada do gatilho ao FDA. Toda vez que uma avalanche acontecer, seu sinal é amplificado e formatado em um pulso TTL que é lido por um contador.

A fim de determinar P_D experimentalmente, procedemos da seguinte forma: com o laser desligado, pulsos de gatilho foram enviados com frequência f (10kHz). Mediu-se o número de contagens de escuro, N_{escuro} , detectados durante um tempo T_i . O produto fT_i dá o número de pulsos gatilhos enviados durante a medição. A probabilidade de contagem de escuro, P_D , é dada por

$$P_D = N_{escuro} / T_i f . \quad (4.2)$$

Para determinar a eficiência quântica, procedeu-se de forma semelhante ao anterior, mas agora com o laser ligado. Mediu-se, portanto, o número de contagens com luz, N_{luz} . A probabilidade de contagem com luz e a eficiência quântica são, respectivamente,

$$P_{luz} = N_{luz} / T_i f \quad (4.3)$$

$$\eta = \ln \left\{ \left[\frac{(1 - P_D)}{(1 - P_{luz})} \right]^{\frac{1}{\langle n \rangle}} \right\} . \quad (4.4)$$

Como se pode observar de (4.4), é necessário estimar o número médio de fótons de um pulso chegando ao FDA. Isto pode ser feito medindo a energia do pulso na saída do laser. Para esta tarefa, foi utilizado o receptor óptico com fotodiodo PIN apresentado no Capítulo 8. A forma do pulso na saída do receptor óptico é mostrada na Figura 4.5. Com base nessa figura, o valor da energia do pulso óptico medido é dado por

$$E = \frac{1}{R\mathfrak{R}} \int_{-\infty}^{\infty} V dt \approx \langle n \rangle h\nu \Rightarrow \langle n \rangle = \frac{\lambda}{hcR\mathfrak{R}} \int_{-\infty}^{+\infty} V dt , \quad (4.5)$$

em que R (130 Ω) é o resistor de carga do receptor óptico, \mathfrak{R} (=0,9) é a responsividade do fotodiodo PIN em 1550nm da Thorlabs, h é a constante de Planck, λ é o comprimento de onda, c é a velocidade da luz no vácuo e V é o pulso de tensão mostrado na Figura 4.5. O

valor encontrado para o número médio de fótons dos pulsos emitidos pelo laser foi $\langle n \rangle \approx 1,9993 \times 10^7$.

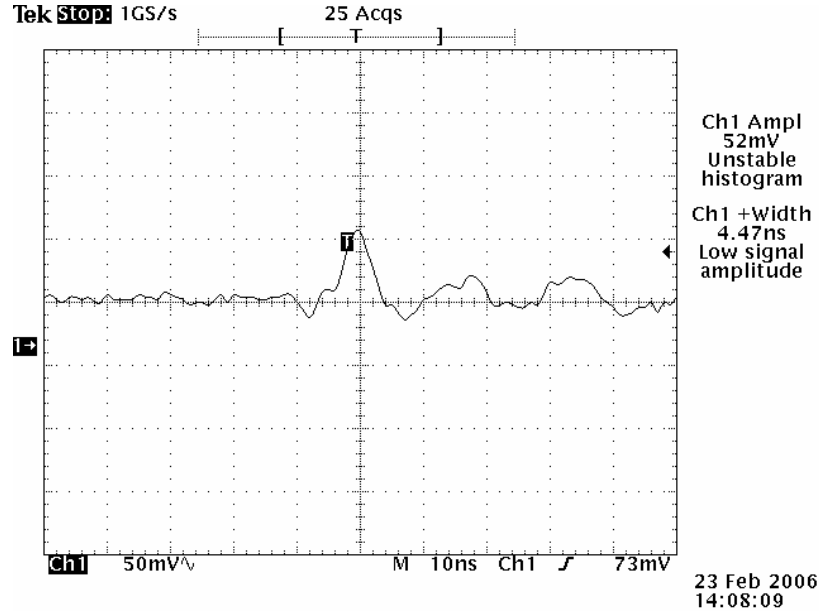


Figura 4.5: Pulso elétrico gerado na saída do fotodetector PIN devido à detecção do pulso óptico emitido pelo diodo laser.

Dois FDAs C30645E (InGaAs/PerkinElmer) denominados a e b foram testados. Para a temperatura de aproximadamente -45°C e $V_{FDA}=38,5\text{V}$, obteve-se $P_{Da}=0,05443$ e $P_{Db}=0,0292$ [33]. As probabilidades de detecção medidas para ambos os FDAs com o laser ligado estão na Figura 4.6 [33]. Na mesma figura existem duas curvas contínuas que representam a probabilidade de detecção que foram obtidas usando a probabilidade de contagem de escuro medidas e a expressão

$$P_{\text{Detecção}} = 1 - \exp(-\eta \langle n \rangle) (1 - P_D). \quad (4.6)$$

Na equação (4.6), o valor do número médio de fótons usado foi $1,99 \times 10^7 \times 10^{-\alpha[\text{dB}]/10}$, em que α é a perda em dB determinada no atenuador variável. Comparando as curvas na Figura 4.6, podemos observar que a eficiência do FDA_a (0,2%) foi menor que eficiência do FDA_b (0,6%).

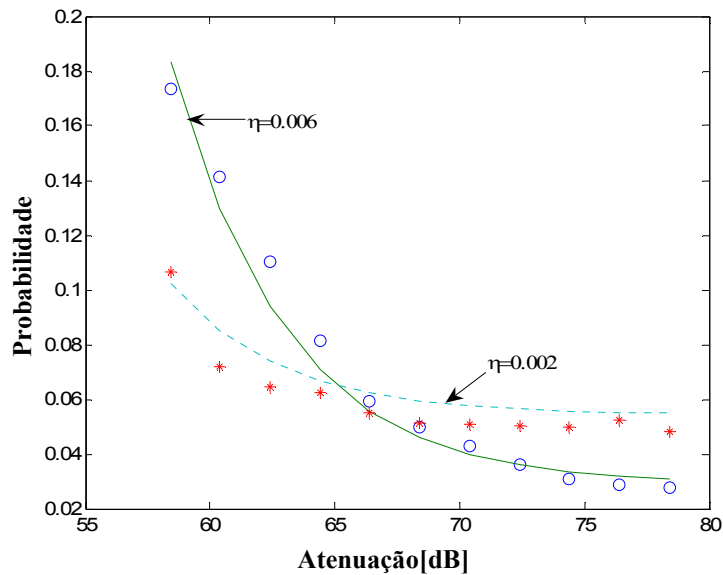


Figura 4.6: Probabilidade de detecção no FDA_a (*) e FDA_b(o) versus atenuação.

Na Figura 4.7 é mostrada uma fotografia do DFI microcontrolado com o sistema de resfriamento usando elementos *Peltier* [33]. Na placa estão juntos o detector de fótons isolados propriamente dito, gerador de pulsos, gerador de atraso e interface RS232 para comunicação e controle com o PC.

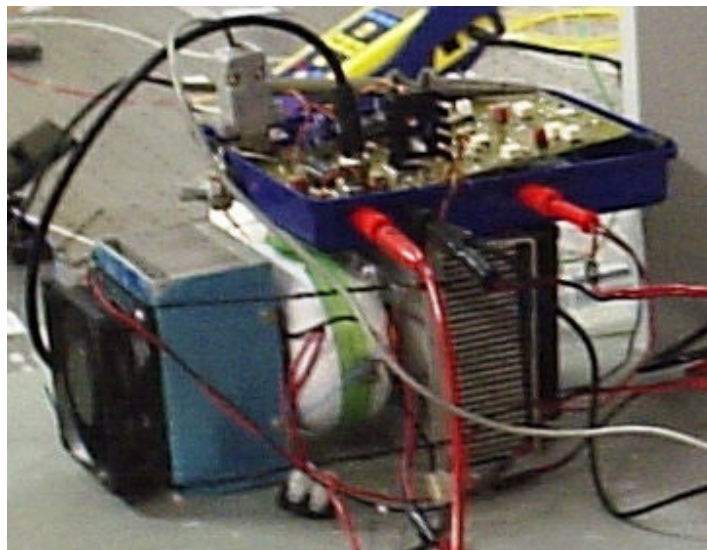


Figura 4.7: Detector de fótons isolados desenvolvido no LATIQ/UFC.

4.2 Resultados Experimentais do Sistema de DQC executando o Protocolo B92

No LATIQ foi desenvolvido o mais simples sistema de DQC que pode ser realizado, que é o que executa o protocolo B92 usando polarização de pulsos coerentes fracos. Foi necessário para sua realização um diodo laser e seus controladores de corrente (*CLC*) e temperatura (*TLC*), dois detectores de fótons isolados (*DFI*) que foram apresentados na seção anterior, dois divisores feixes por polarização (*PBS*), uma chave eletro-óptica (*EOS*), dois acopladores balanceados (*BS*), dois rotacionadores de polarização (*P*), um atenuador variável (*A*) e, como canal, foram utilizados três rolos de fibra óptica que resultam num comprimento de 200m. A configuração do esquema óptico está mostrada na Figura 4.8.

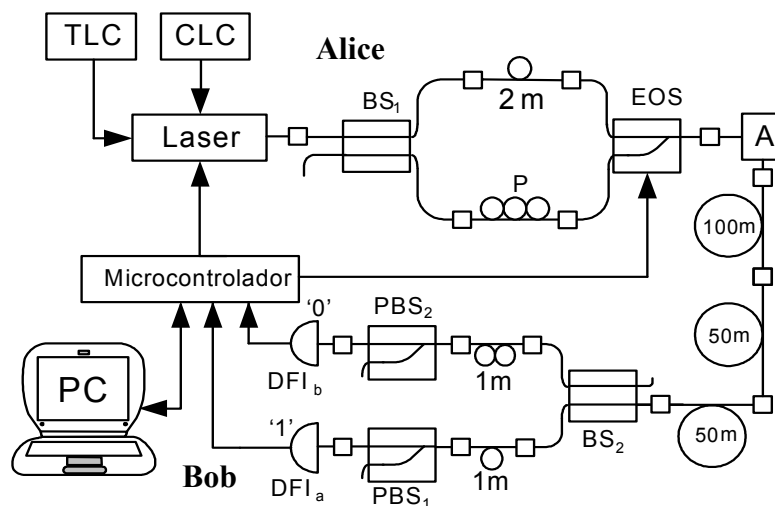


Figura 4.8: Configuração óptica utilizada na implementação do sistema de DQC polarimétrico executando o protocolo B92.

Inicialmente, o PC envia ao PIC a seqüência de bits aleatória, conforme regras do protocolo B92, que Alice deve enviar. Para cada valor de bit, o PIC envia um pulso elétrico a fim de selecionar a polarização $|0\rangle$ (braço superior) para o bit 0, ou $|\frac{\pi}{4}\rangle$ (braço inferior) para o bit 1. O pulso óptico é então atenuado por *A* e enviado para Bob através de um enlace de fibra óptica. Em Bob, o pulso é dividido pelo acoplador *BS*₂. Metade dele vai para o *PBS*₁ e a outra metade para o *PBS*₂. Antes disso, eles passam por um rotacionador de polarização composto por dois rolos de fibra de 1m cada. Se um pulso com polarização $|0\rangle$ foi enviado,

haverá a possibilidade de ele ser detectado (idealmente) apenas pelo DFI_b . No entanto, se um pulso com polarização $|\frac{\pi}{4}\rangle$ foi enviado, haverá a possibilidade de ele ser detectado, também idealmente, apenas pelo DFI_a . O controle do sistema é realizado por um software também desenvolvido no LATIQ, cuja aparência visual está mostrada na Figura 4.10.



Figura 4.9: Foto da configuração óptica utilizada na implementação do sistema de DQC polarimétrico executando o protocolo B92.

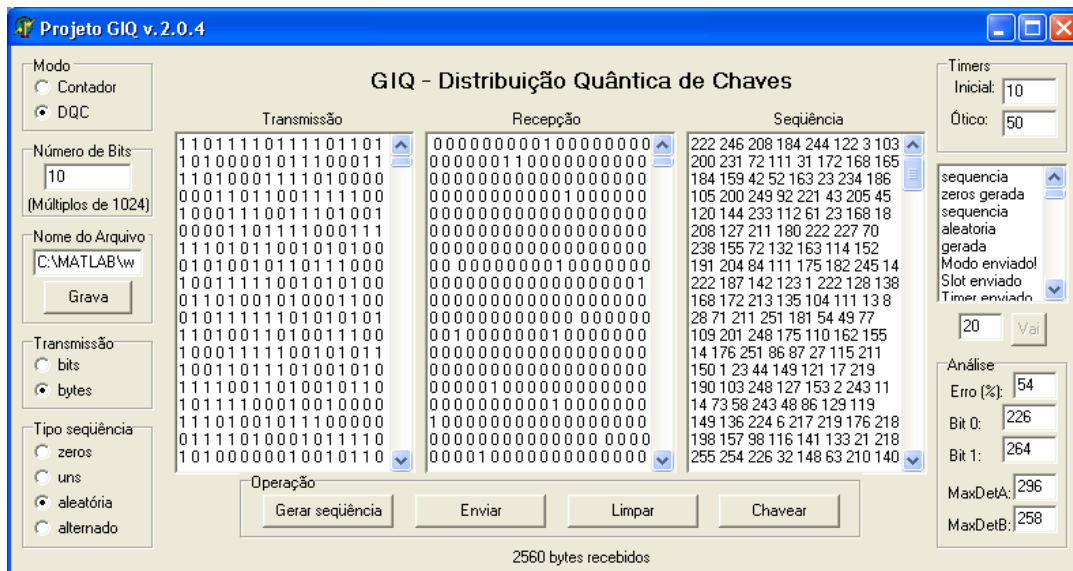


Figura 4.10: Tela do software que controla o sistema de DQC.

O sistema foi testado para dois diferentes conjuntos de valores de parâmetros. No primeiro caso, foi usado o mesmo pulso de gatilho mostrado na Figura 4.2, tendo ele uma largura $\tau_g \approx 6,825\text{ns}$ e amplitude $V_g \approx 3,43\text{V}$. Os FDAs foram mantidos sob temperatura $T \approx -45^\circ\text{C}$ e tensão $V_{FDA} = 40,5\text{V}$. Inicialmente, apenas bits 0 foram enviados, depois apenas bits 1 e, por fim, uma seqüência aleatória de bits. Para cada situação a atenuação foi variada em passos de 2dB. As Figuras 4.11 e 4.12 mostram as curvas de probabilidade de detecção em DFI_a e DFI_b , respectivamente, quando somente bits 1 (*) e bits 0 (.) foram enviados. Nelas, também estão as curvas de eficiência (linhas contínuas) para cada um dos detectores.

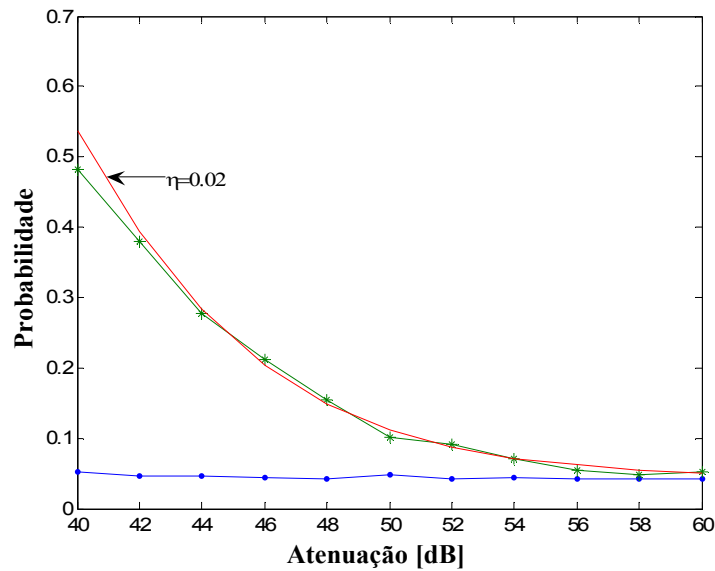


Figura 4.11: Probabilidade de detecção no DFI_a quando foram enviados apenas bits 1 (*) e apenas bits 0 (.) com o conjunto de parâmetros $V_g=3,43\text{V}$, $\tau_g=6,825\text{ns}$, $V_{FDA}=40,5\text{V}$ e $T \approx -45^\circ\text{C}$. $P_{Da}=0,04419$ e $NEP_a = 23,075 \times 10^{-13} \text{J}/\sqrt{\text{Hz}}$.

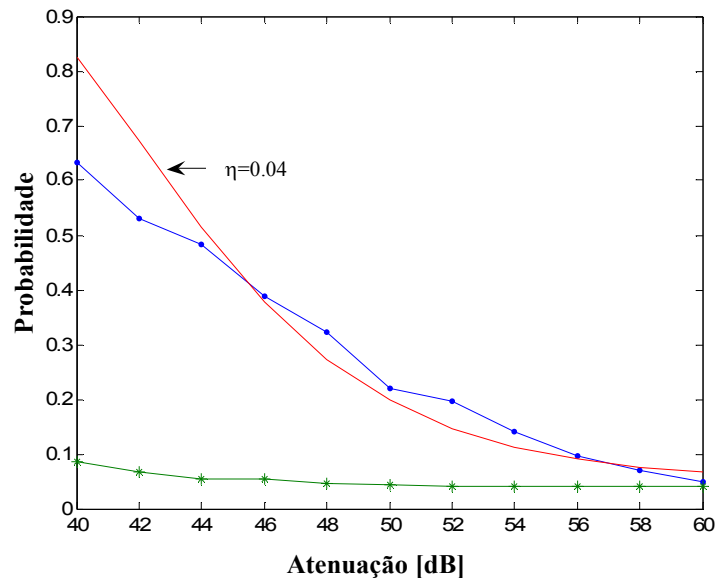


Figura 4.12: Probabilidade de detecção no DFI_b quando foram enviados apenas bits 0 (.) e apenas bits 1 (*) com o conjunto de parâmetros $V_g=3,43V$, $\tau_g=6,825ns$, $V_{FDA}=40,5V$ e $T\approx-45^\circ C$. $P_{Da}=0,05005$ e $NEP_b=12,278\times 10^{-13} J/\sqrt{Hz}$.

Para estes novos parâmetros, as medidas de eficiência foram 2% para o DFI_a e 4% para o DFI_b . O aumento dos valores obtidos em relação aos mostrados na Figura 4.6 é devido ao aumento do valor de V_{FDA} . Como esperado, para ambos DFIs, com o aumento da atenuação, probabilidade de detecção diminuiu. As probabilidades não nulas de detecção no DFI_a e DFI_b quando bit 0 e bit 1 foram enviados, respectivamente, são devidos às contagens de escuro. As probabilidades de escuro médias obtidas foram $P_{Da}=0,04419$ e $P_{Db}=0,05005$. O número médio de fótons por pulso chegando aos detectores DFI_a para cada valor de atenuação no intervalo de 40dB e 60dB quando bits 1 foram enviados é $\{36,24, 22,86, 14,43, 9,10, 5,74, 3,62, 2,29, 1,44, 0,91, 0,57, 0,362\}$. Já para DFI_b , o número médio de fótons por pulso chegando a ele quando bits 0 foram enviados é $\{25,01, 15,78, 9,96, 6,28, 3,96, 2,50, 1,58, 0,995, 0,628, 0,396, 0,250\}$. A taxa de erro quando apenas são enviados bits 0 (o) e bits 1 (*) é mostrada na Figura 4.13.

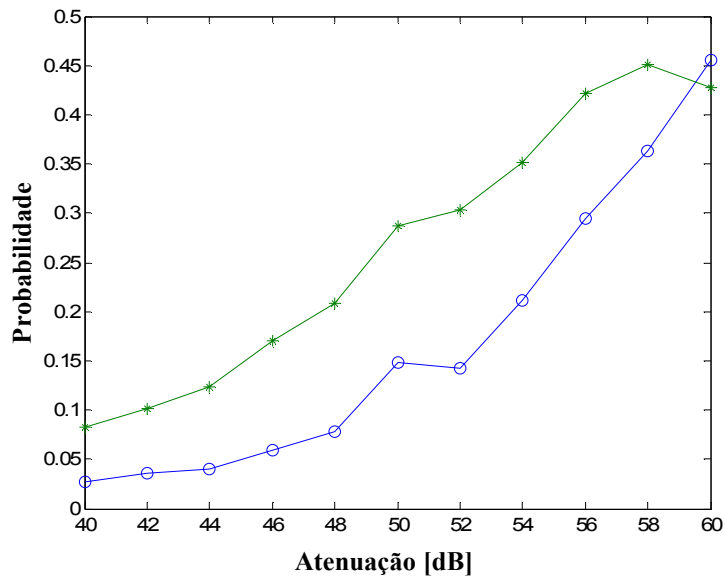


Figura 4.13: Taxa de erro versus atenuação quando são enviados apenas bits 0 (o) e apenas bits 1 (*).

Como era de se esperar, com o aumento da atenuação, a taxa de erro tende para o valor de 50%. Na Figura 4.14 são mostradas curvas das probabilidades de detecção para ambos DFIs (o,*) e para a taxa de erro (□) quando uma seqüência aleatória de bits é enviada por Alice.

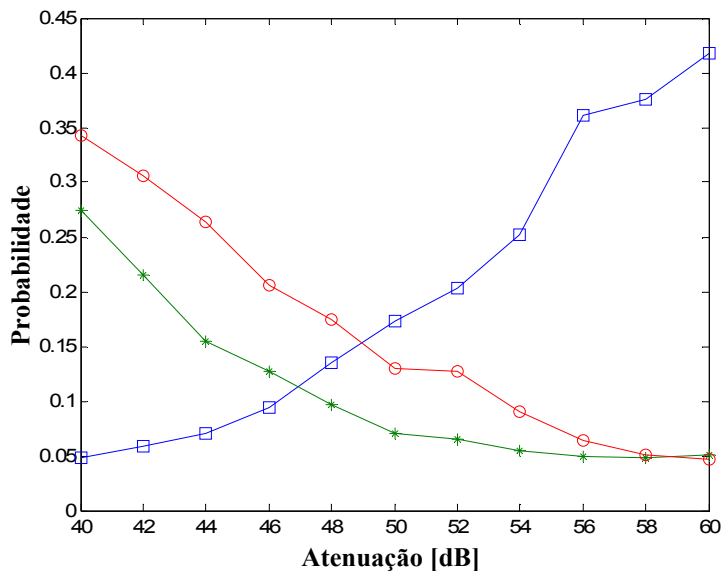


Figura 4.14: Probabilidade de detecção no DF_{I_a} (o), DF_{I_b} (*) e a taxa de erro (□) quando uma seqüência aleatória de bits é enviada por Alice.

Uma vez que bits 0 e 1 ocorrem com a mesma probabilidade, detecções deveriam ocorrer nos detectores DFI_a e DFI_b com a mesma frequência. No entanto, como $\eta_b > \eta_a$, mais contagens são observadas no DFI_b , fazendo com que a sequência final obtida contenha mais bits 0 que bits 1. Numa segunda situação, utilizou-se $V_{FDA}=41V$ e $\tau_g \approx 9ns$. As probabilidades de contagens de escuro são $P_{Da} = 0,08702$ e $P_{Db} = 0,10548$. As Figuras 4.15-4.17 mostram os resultados obtidos. Como os valores de V_{FDA} e τ_g são maiores que os usados no primeiro caso mostrado anteriormente, a eficiência e a probabilidade de contagem também são maiores. A eficiência do DFI_a tende para 4% (Figura 4.15), enquanto a eficiência do DFI_b tende para 7,5% (Figura 4.16). Na primeira situação, os valores de NEP para ambos DFIs foram: $NEP_a = 23,075 \times 10^{-13} J/\sqrt{Hz}$ e $NEP_b = 12,278 \times 10^{-13} J/\sqrt{Hz}$. Já na segunda, $NEP_a = 14,099 \times 10^{-13} J/\sqrt{Hz}$ e $NEP_b = 8,278 \times 10^{-13} J/\sqrt{Hz}$. Portanto os parâmetros usados na segunda situação são melhores que os da primeira.

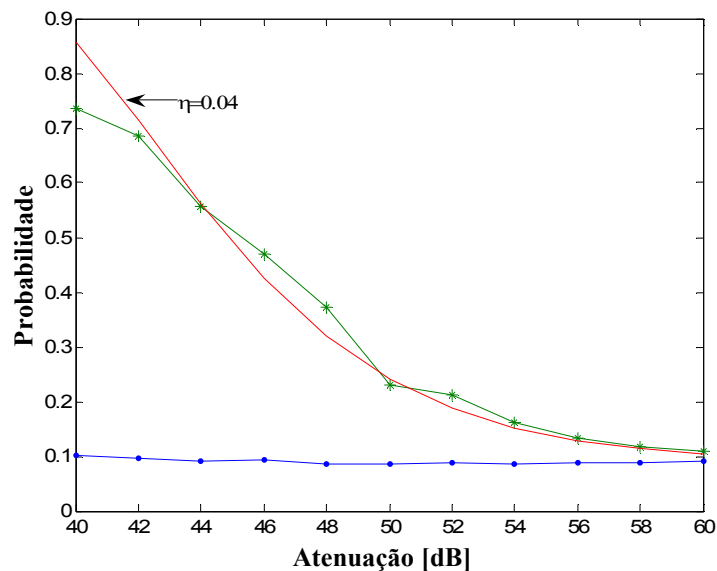


Figura 4.15: Probabilidade de detecção no DFI_a quando são enviados apenas bits 0 (*) e apenas bits 1 (.) com o conjunto de parâmetros $V_g=3,43V$, $\tau_g=9ns$, $V_{FDA}=41V$ e $T \approx 45^\circ C$. $P_{Da}=0,08702$ e $NEP_a=14,099 \cdot 10^{-13} J/Hz^{1/2}$.

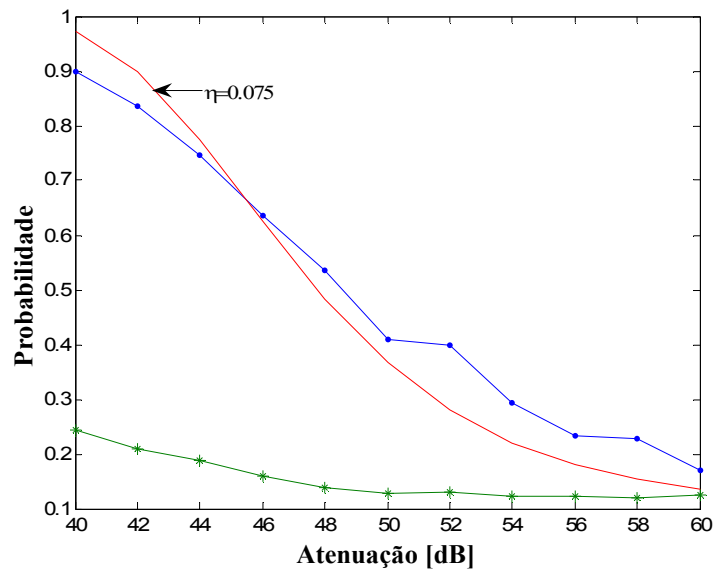


Figura 4.16: Probabilidade de detecção no DFI_b quando forma enviados apenas bits 0 (*) apenas bits 1 (.) com o conjunto de parâmetros $V_g=3,43V$, $\tau_g=9ns$, $V_{FDA}=41V$ e $T\approx 45^\circ C$. $P_{Db}=0,10548$ e $NEP_b=8,278.10^{-13}J/Hz^{1/2}$.

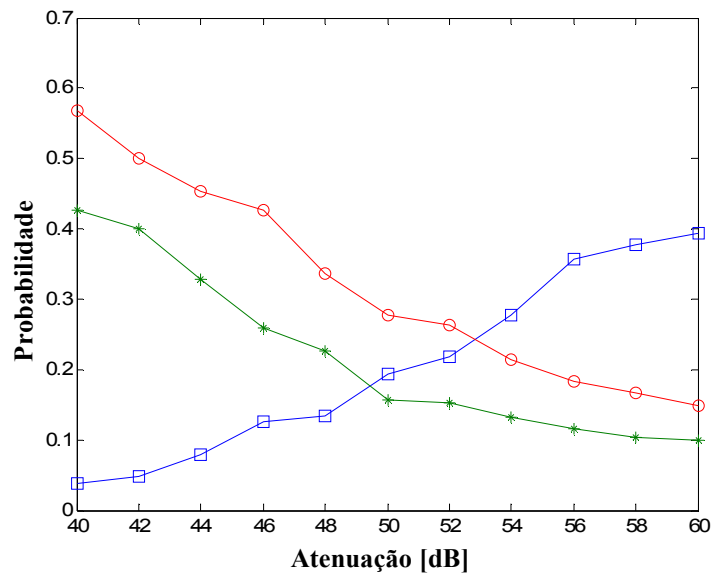


Figura 4.17: Probabilidade de detecção no DFI_a (*), DFI_b (.) e a taxa de erro (□) quando uma seqüência aleatória de bits é enviada por Alice com os parâmetros $V_g=3,43V$, $\tau_g=9ns$, $V_{FDA}=41V$ e $T\approx 45^\circ C$. $P_{Da}=0,08702$ e $NEP_a=14,099\times 10^{-13}J/\sqrt{Hz}$. $P_{Db}=0,10548$ e $NEP_b=8,278\times 10^{-13}J/\sqrt{Hz}$.

Capítulo 5

ENCRIPÇÃO FÍSICA COM ESTADOS COERENTES MESOSCÓPICOS

Neste capítulo é apresentado um sistema de encriptação física de dados usando estados coerentes mesoscópicos. Um estado coerente de luz mesoscópico pode ser entendido como um estado coerente que fica na fronteira entre os conceitos que abrangem a física clássica e a física quântica. Será mostrado que, para esse protótipo de encriptação de mensagens, a segurança é garantida graças ao ruído quântico próprio dos estados coerentes. Além disso, será mostrado que o nível de segurança do sistema é dado em função dos parâmetros $\langle n \rangle$ (número médio de fótons) e M (número de bases de codificação) de cada pulso mesoscópico enviado.

5.1 Estados Coerentes

Os estados coerentes são estados que possuem distribuição Poissoniana do número de fótons. Tal característica os possibilita ter uma fase mais bem definida que os estados número, os quais possuem fase totalmente aleatória. Além disso, o produto de incerteza é o mínimo permitido pelo princípio da incerteza de Heisenberg [34]

$$\Delta p \Delta q = \frac{\hbar}{2}. \quad (5.1)$$

Os estados coerentes podem ser gerados usando operador $D(\alpha) = \exp(\alpha a^\dagger - \alpha^* a)$ aplicado ao estado vácuo $|0\rangle$, o que define a expressão do estado coerente em função de estados números como sendo [34]

$$|\alpha\rangle = e^{(\alpha a^\dagger - \alpha^* a)} |0\rangle = e^{\alpha a^\dagger} e^{\alpha^* a} e^{-|\alpha|^2/2} |0\rangle = e^{-\frac{|\alpha|^2}{2}} \sum_{n=0}^{\infty} \frac{\alpha^n}{\sqrt{n!}} |n\rangle, \quad (5.2)$$

em que a^\dagger e a são os operadores criação e aniquilação, respectivamente. Com base na equação (5.2), podem-se listar algumas propriedades importantes dos estados coerentes:

(a) O número médio de fótons do estado $|\alpha\rangle$ é dado por

$$\langle n \rangle = \langle \alpha | a^\dagger a | \alpha \rangle = |\alpha|^2. \quad (5.3)$$

(b) A probabilidade de encontrarmos n fótons em $|\alpha\rangle$ é dado pela distribuição Poissoniana

$$p(n) = \langle n | \alpha \rangle \langle \alpha | n \rangle = \frac{\langle n \rangle^n e^{-\langle n \rangle}}{n!}. \quad (5.4)$$

Na Figura 5.1 é mostrado $p(n)$ versus n para três diferentes valores de $|\alpha|^2$.

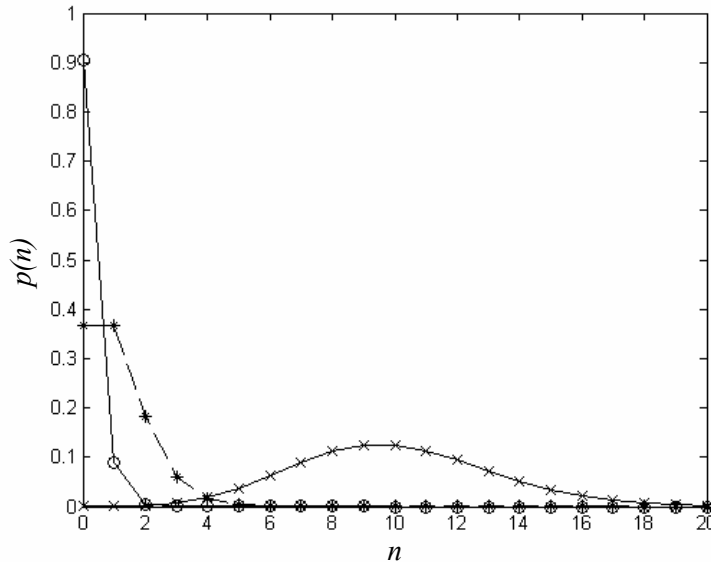


Figura 5.1: Distribuição do número de fótons $p(n)$ versus número de fótons n para estados coerentes com $|\alpha|^2=0,1(\mathbf{o})$, $|\alpha|^2=1(*)$ e $|\alpha|^2=10(\mathbf{x})$.

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

$$\frac{1}{\pi} \int |\alpha\rangle \langle \alpha| d^2\alpha = 1 \quad (5.5)$$

(d) Dois estados coerentes correspondentes a dois auto-estados diferentes α e β são não ortogonais, assim

$$\langle \alpha | \beta \rangle = \exp \left[-\frac{1}{2} (|\alpha|^2 + |\beta|^2) + \beta \alpha^* \right] \quad (5.6)$$

$$|\langle \alpha | \beta \rangle|^2 = \exp(-|\alpha - \beta|^2). \quad (5.7)$$

De (5.7), se a magnitude de $\alpha - \beta$ é muito maior que a unidade, os estados são aproximadamente ortogonais.

5.2 Parâmetros de Stokes

Em óptica clássica, o estado de polarização de um feixe de luz pode ser descrito como um vetor de Stokes na esfera de Poincaré, como mostrado na Figura 5.2. Ele pode ser completamente caracterizado pelos quatro parâmetros clássicos de Stokes [35,36]

$$S_0 = |\alpha_1|^2 + |\alpha_2|^2 \quad (5.8)$$

$$S_1 = |\alpha_1|^2 - |\alpha_2|^2 \quad (5.9)$$

$$S_2 = (\alpha_1^* \alpha_2 + \alpha_1 \alpha_2^*) \quad (5.10)$$

$$S_3 = -i(\alpha_1^* \alpha_2 - \alpha_1 \alpha_2^*), \quad (5.11)$$

em que S_0 mede a intensidade do feixe e S_1 , S_2 e S_3 caracterizam sua polarização. O raio da esfera é dado por

$$S = \sqrt{S_1^2 + S_2^2 + S_3^2}, \quad (5.12)$$

que define a intensidade média da parte polarizada da radiação. O grau de polarização é dado por S/S_0 . De forma semelhante, os operadores quânticos de Stokes são definidos como sendo [35,36]

$$\hat{S}_0 = \hat{a}_1^\dagger \hat{a}_1 + \hat{a}_2^\dagger \hat{a}_2, \quad (5.13)$$

$$\hat{S}_1 = \hat{a}_1^\dagger \hat{a}_1 - \hat{a}_2^\dagger \hat{a}_2, \quad (5.14)$$

$$\hat{S}_2 = \hat{a}_1^\dagger \hat{a}_2 + \hat{a}_2^\dagger \hat{a}_1, \quad (5.15)$$

$$\hat{S}_3 = -i(\hat{a}_1^\dagger \hat{a}_2 - \hat{a}_2^\dagger \hat{a}_1) \quad (5.16)$$

$$[\hat{a}_i, \hat{a}_j^\dagger] = 1, \quad i, j = 1, 2, \quad (5.17)$$

em que (5.17) define a relação de comutação usual que os operadores $\hat{a}_1^\dagger(\hat{a}_1)$ e $\hat{a}_2^\dagger(\hat{a}_2)$ devem satisfazer. Como base nisso, os valores médios dos parâmetros quânticos de Stokes de um estado coerente $|\alpha_1, \alpha_2\rangle$ tem valores idênticos aos mostrados nas equações 5.8-5.11 para os clássicos. No entanto, os parâmetros quânticos exibem flutuações que são expressas por suas variâncias [35,36]

$$V_i \equiv \langle (\Delta \hat{S}_i)^2 \rangle = \langle \hat{S}_i^2 \rangle - \langle \hat{S}_i \rangle^2, \quad i = 0, 1, 2, 3, \quad (5.18)$$

$$\langle \hat{S}_i^x \rangle = \langle \alpha_1 \alpha_2 | \hat{S}_i^x | \alpha_1 \alpha_2 \rangle, \quad x = 1, 2. \quad (5.19)$$

Portanto, em vez de um ponto na esfera de Poincaré, um estado coerente é definido por uma distribuição de probabilidade de estados na superfície da esfera como mostrado na Figura 5.2. É fácil demonstrar usando (5.13)-(5.17) que os parâmetros de Stokes obedecem às seguintes relações de comutação

$$[\hat{S}_i, \hat{S}_j] = 2i\hat{S}_k, \quad i, j, k = 1, 2, 3 \quad (5.20)$$

$$[\hat{S}_0, \hat{S}_i] = 0, \quad i = 1, 2, 3. \quad (5.21)$$

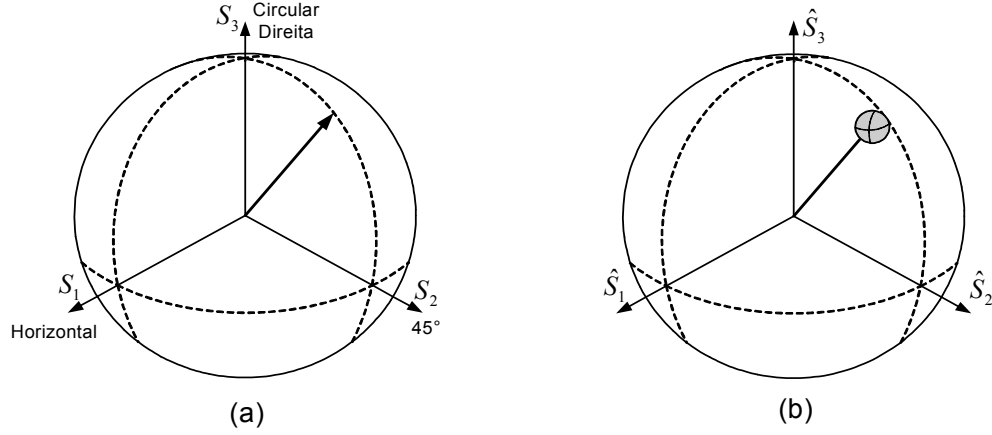


Figura 5.2: Diagrama do vetor de Stokes clássico (a) e quântico (b) mapeados na esfera de Poincaré. A bola no final do vetor representa o ruído quântico nos operadores \hat{S}_1 , \hat{S}_2 e \hat{S}_3 .

Diretamente, (5.20) mostra que não é possível saber, com total certeza, qualquer par de parâmetros simultaneamente. Por fim, pode ser demonstrado, com base em (5.13)-(5.17), que o raio da esfera de Poincaré, considerando os parâmetros de Stokes quânticos, é dada por

$$\langle \hat{S} \rangle = \sqrt{\langle \hat{S}_0^2 \rangle + 2\langle \hat{S}_0 \rangle}. \quad (5.22)$$

Os valores médios e as variâncias dos parâmetros quânticos de Stokes de um estado coerente $|\alpha, \beta\rangle$ ($|\alpha\rangle$ representa a luz polarizada na direção x e $|\beta\rangle$ a luz polarizada na direção y) são dados por

$$|\alpha, \beta\rangle = \sum_{n=0}^{\infty} e^{-\frac{|\alpha|^2}{2}} \frac{\alpha^n}{\sqrt{n!}} |n\rangle \otimes \sum_{k=0}^{\infty} e^{-\frac{|\beta|^2}{2}} \frac{\beta^k}{\sqrt{k!}} |k\rangle \quad (5.23)$$

$$\langle \hat{S}_1 \rangle = |\alpha|^2 - |\beta|^2, \quad \langle \hat{S}_1^2 \rangle = (|\alpha|^2 - |\beta|^2)^2 + |\alpha|^2 + |\beta|^2, \quad V_1 = |\alpha|^2 + |\beta|^2 \quad (5.24)$$

$$\langle \hat{S}_2 \rangle = \alpha^* \beta + \alpha \beta^*, \quad \langle \hat{S}_2^2 \rangle = (\alpha^* \beta)^2 + (\alpha \beta^*)^2 + |\alpha|^2 + |\beta|^2 + 2|\alpha|^2 |\beta|^2, \quad V_2 = |\alpha|^2 + |\beta|^2 \quad (5.25)$$

$$\langle \hat{S}_3 \rangle = i(\alpha^* \beta - \alpha \beta^*), \quad \langle \hat{S}_3^2 \rangle = -(\alpha^* \beta)^2 - (\alpha \beta^*)^2 + |\alpha|^2 + |\beta|^2 + 2|\alpha|^2 |\beta|^2, \quad V_3 = |\alpha|^2 + |\beta|^2 \quad (5.26)$$

De (5.24)-(5.26), pode-se notar que os parâmetros quânticos exibem flutuações que são expressas por suas variâncias. Para estados coerentes, quanto maior a potência luminosa

maior a variância nos três parâmetros. Em geral, para aplicar um deslocamento de fase ϕ entre dois modos linearmente polarizados, é usado o operador unitário [35,36]:

$$U_\phi = \exp(i0.5\phi\hat{S}_1). \quad (5.27)$$

Por exemplo, quando U_ϕ é aplicado ao estado coerente $|\alpha, \beta\rangle$, o resultado é $|\alpha e^{i\phi/2}, \beta e^{-i\phi/2}\rangle$.

Por outro lado, uma rotação geométrica de θ na polarização pode ser obtida pela aplicação do operador unitário:

$$U_\theta = \exp(i\theta\hat{S}_3). \quad (5.28)$$

Assim, $U_\theta |\alpha, 0\rangle$ resulta em $|\alpha \cos \theta, \alpha \sin \theta\rangle$.

Classicamente, um pulso de luz é despolarizado se seus parâmetros de Stokes se anulam. No entanto, do ponto de vista quântico, esta condição é necessária, mas não suficiente. Um feixe de luz pode ser considerado despolarizado se suas propriedades observáveis permanecem inalteradas depois da aplicação de uma rotação geométrica e/ou deslocamento de fase entre duas componentes polarizadas linearmente. Esta condição é descrita matematicamente por [37]:

$$[\rho, \hat{S}_3] = [\rho, \hat{S}_1] = 0. \quad (5.29)$$

A forma geral de um estado despolarizado é dado por [38,39]

$$\rho = \sum_n p_n \frac{1}{n+1} \sum_{k=0}^n |n\rangle |n-k\rangle \langle k| \langle n-k|, \quad (5.30)$$

em que p_n é a função de distribuição de probabilidade do número de fótons considerando ambos modos.

5.3 Descrição do Sistema de Encriptação Física com Estados Coerentes Mesoscópicos

Os protocolos de comunicação seguros protegidos pelas leis da mecânica quântica em vez de complexidade matemática como, por exemplo, os protocolos BB84 e B92, parecem ter encontrado um gargalo que atrasa suas aplicações em redes de comunicações reais. O mesmo teorema da não clonagem que garante a segurança proíbe a amplificação de sinal necessário em redes de comunicação de longa distância. Isto implica, em termos práticos, à limitação da taxa de transmissão líquida dos bits da seqüência da chave e o alcance do sistema [40].

O sistema de encriptação a ser discutido é associado a um processo em que mensagens são enviadas de forma segura de Alice para Bob, sendo usada, para tal propósito, uma chave inicial K_0 que é obtida a partir da expansão apropriada por algoritmo duma chave K secreta de menor comprimento [40-43]. Além disso, K e K_0 devem ser usadas apenas uma vez e nunca são divulgadas publicamente. A principal razão para isto é que, num possível ataque de espionagem, uma linha de atraso pode ser criada de tal forma que um espião realize suas medições nos estados em que ele interceptou apenas quando a chave usada for divulgada. Portanto, isso permitiria extrair informação precisamente assim como os usuários legítimos fazem [43].

Os principais elementos usados na implementação do sistema e, também, um possível aparato que pode ser usado num ataque de espionagem estão esboçados na Figura 5.3 [43]. Os dois usuários estão conectados através de um canal óptico de comunicação que pode ser fibra óptica ou espaço livre. Os moduladores ópticos podem efetuar modulação na polarização ou fase de um pulso de luz coerente e, logicamente, o sistema de detecção deve ser sensível ao tipo de modulação escolhido. Na implementação, apenas dispositivos de telecomunicações disponíveis comercialmente são considerados e, ademais, o sistema tem como propósito ser de baixo custo e comercialmente atrativo. Alice possui um computador que controla um sistema de geração de pulsos de luz mesoscópicos, um modulador óptico que executa uma modulação específica dentro do total de M bases do protocolo, conforme um valor aleatório k [$k=0, 1, \dots, (M-1)$], e um pseudo-gerador de números aleatórios (PGNA) que gera efetivamente a seqüência de bits da mensagem R a ser transmitida.

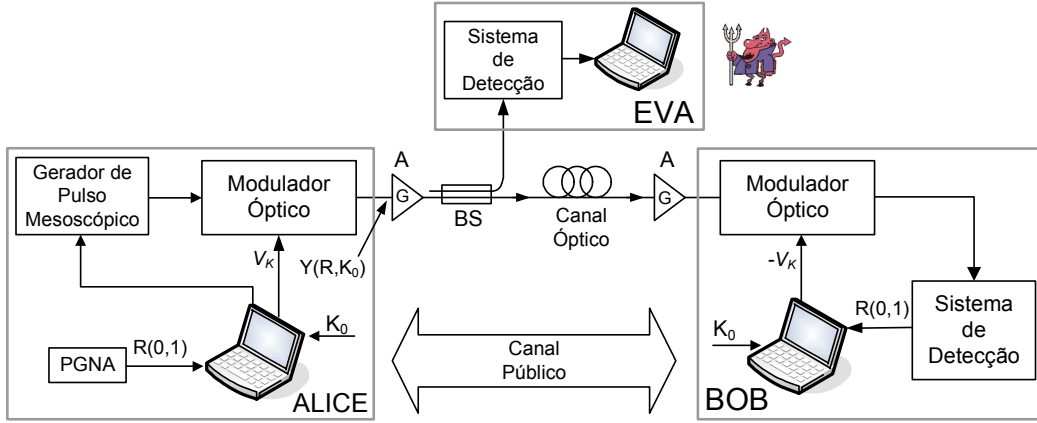


Figura 5.3: Esquema básico para implementação de protocolos de comunicação quântica usando estados coerentes mesoscópicos. A - amplificador óptico com ganho G , V - sinal elétrico para modulação dos pulsos mesoscópicos.

A Figura 5.4 ilustra como fica a representação dos círculos de codificação de fase na esfera de Poincaré com número de bases M variando de 1 a 5 [43].

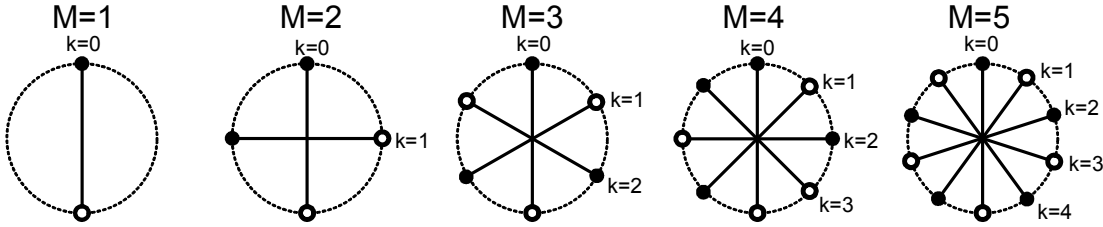


Figura 5.4: Círculo de codificação para ângulos de fase ϕ_k para $M=1$ a $M=5$. Cada valor de k especifica uma base de dois estados, defasados de π , que representam o bit 0 (o) e o bit 1 (•).

Conforme está mostrado na Figura 5.4, para uma base com k par, o bit ‘0’ é definido pelo ângulo de fase total $\phi = \phi_k + 0$ enquanto que o bit ‘1’, na mesma base, é definido por $\phi = \phi_k + \pi$. Por outro lado, para uma base ímpar, acontece o contrário: o bit ‘0’ é definido por $\phi = \phi_k + \pi$ e o bit ‘1’ por $\phi = \phi_k + 0$. No caso da codificação de polarização, para k par, o bit ‘0’ é definido pelo ângulo de polarização $\theta = \theta_k + 0$ enquanto que o bit ‘1’, na mesma base, é definido por $\theta = \theta_k + \pi/2$. Por outro lado, para uma base ímpar, o bit ‘0’ é definido por $\theta = \theta_k + \pi/2$ e o bit ‘1’ por $\theta = \theta_k + 0$. Deste modo, todos os ângulos adjacentes para M ímpar apresentam um padrão de alternância dos valores dos bits para cada base. Isto

indica que, para uma aplicação que utiliza um número de bases suficientemente grande, um pequeno erro na medição pode causar um equívoco. Esse é o princípio básico em que se baseia a segurança desse sistema [43]. A estrutura do círculo de codificação pode ser conhecida por um espião, mas não o bit e a seqüência de base usada na codificação de cada bit emitido. Como descrito em [41-43], o número de bases M usadas e o número médio de fótons $\langle n \rangle$ devem ser escolhidos de tal forma que um determinado nível de segurança seja alcançado.

Considere que o sinal a ser enviado de Alice para Bob foi devidamente preparado contra possíveis ataques de um espião logo na saída de Alice. Este sinal é então enviado para Bob através de um canal óptico com perdas. Um segundo ponto importante desse sistema é que ele não detecta a presença de intrusos e, portanto, pode-se assumir que Eva pode copiar com total precisão o sinal enviado para Bob. Desse modo, a estação de Eva pode estar localizada em qualquer ponto do canal, mas o melhor ponto para ela é logo na saída de Alice, em que não ocorreu nenhum tipo de perda causada pelo canal. Uma maneira simples de preparar uma cópia do sinal com a mesma potência é usar um amplificador óptico que duplica a potência do sinal a ser interceptado e, logo após, um divisor de feixes (BS) 50/50 que guia metade do sinal para Bob e outra metade para Eva. Os dois sinais na saída do divisor de feixes são iguais.

A habilidade de Bob para extrair sinais com boa relação sinal ruído diminui com a distância, pois o canal apresenta perdas. Sendo assim, amplificadores ópticos podem ser adicionados em aplicações de longa distância para contornar tal problema, mas, além disso, eles também introduzem ruído. Portanto, a teoria da informação diz que se a informação mútua I_{AB} entre Alice e Bob é menor que a entre Alice e Eva, I_{AE} , o sistema não apresenta nível de segurança desejado. Por outro lado, $I_{AB} > I_{AE}$ indica que a segurança pode ser alcançada com o sistema apresentado [43].

De forma geral, o protocolo obedece aos seguintes passos:

- i – Alice e Bob compartilham uma seqüência aleatória secreta inicial contendo K bits que deve ser usada apenas uma única vez e nunca deve ser feita pública. Ambos expandem por algoritmo essa chave numa chave K_0 . Essa seqüência expandida K_0 é

- quem determina o valor de k (que define a base) a ser usado na modulação dos pulsos;
- ii – Alice gera a mensagem R ;
 - iii – Alice envia para Bob a mensagem R . Cada bit de R é codificado com a base $k(=0,1,\dots,M-1)$;
 - iv – Por conhecer K_θ , Bob decodifica a seqüência de sinais e obtém R ;
 - v – Alice e Bob permanecem nos passos (ii), (iii) e (iv) até consumirem totalmente os bits de K_θ . Dependendo da necessidade ou não, retornam ao ponto (i);
 - vi – Por fim, Alice e Bob aplicam algum método de correção de erro clássico para compartilharem a seqüência de bits que será a mensagem final compartilhada.

Dado que o protocolo foi descrito, a análise a ser feita a partir daqui abrange ambas as modulação de fase e polarização. No caso de estados de polarização, a informação é codificada em dois modos de polarização ortogonais. Considerando, por exemplo, um estado coerente com amplitude α definido por $|\psi_0\rangle = |\alpha, 0\rangle$, ele pode ser “rotacionado” pela aplicação da transformação unitária $U_{\theta_{bv}} = \exp\left[i(\theta_b + \theta_v)\hat{S}_3\right]$. O ângulo θ_v corresponde ao ângulo da base definido pelo protocolo e θ_b ($= 0$ ou $\pi/2$) corresponde ao ângulo do bit a ser transmitido. Logo,

$$|\psi_{bv}\rangle = U_{\theta_{bv}} |\alpha, 0\rangle = |\alpha \cos(\theta_b + \theta_v), \alpha \sin(\theta_b + \theta_v)\rangle. \quad (5.31)$$

No caso de codificação de fase, o estado coerente $|\alpha\rangle$ é dividido em um estado coerente de dois modos

$$|\psi_0\rangle = \left|\frac{\alpha}{\sqrt{2}}\right\rangle_1 \otimes \left|\frac{\alpha}{\sqrt{2}}\right\rangle_2. \quad (5.32)$$

Nesse caso, a codificação é realizada pela aplicação da transformação unitária $U_{\phi_{bv}} = \exp\left[i0.5(\phi_b + \phi_v)\hat{S}_1\right]$ ao estado de (5.32), resultando em

$$|\Psi_{b\nu}\rangle = U_{\phi_{b\nu}} \left| \frac{\alpha}{\sqrt{2}} \right\rangle_1 \otimes \left| \frac{\alpha}{\sqrt{2}} \right\rangle_2 = \left| e^{-i(\phi_b + \phi_\nu)/2} \frac{\alpha}{\sqrt{2}} \right\rangle_1 \otimes \left| e^{i(\phi_b + \phi_\nu)/2} \frac{\alpha}{\sqrt{2}} \right\rangle_2, \quad (5.33)$$

em que $\phi_b (= 0 \text{ ou } \pi)$. Com base nos estados definidos nas equações (5.31) e (5.33), a superposição entre dois estados coerentes modulados com valores de bases distintas para modulação de polarização e fase são, respectivamente,

$$\begin{aligned} \left| \langle \Psi_{b\nu} | \Psi_{b\mu} \rangle \right|^2 &= \left| \langle \alpha^* \sin(\theta_b + \theta_\nu), \alpha^* \cos(\theta_b + \theta_\nu) | \alpha \cos(\theta_b + \theta_\mu), \alpha \cos(\theta_b + \theta_\mu) \rangle \right|^2 = \\ &= \exp \left[-2 |\alpha|^2 \sin^2 \left(\frac{\theta_\nu - \theta_\mu}{2} \right) \right]. \end{aligned} \quad (5.34)$$

$$\begin{aligned} \left| \langle \Psi_{b\nu} | \Psi_{b\mu} \rangle \right|^2 &= \left| \left\langle \frac{\alpha^*}{\sqrt{2}} e^{i(\phi_b + \phi_\nu)/2}, \frac{\alpha^*}{\sqrt{2}} e^{-i(\phi_b + \phi_\nu)/2} \middle| \frac{\alpha}{\sqrt{2}} e^{-i(\phi_b + \phi_\mu)/2}, \frac{\alpha}{\sqrt{2}} e^{i(\phi_b + \phi_\mu)/2} \right\rangle \right|^2 = \\ &= \exp \left[-2 |\alpha|^2 \left(1 - \cos \left(\frac{\phi_\nu - \phi_\mu}{2} \right) \right) \right]. \end{aligned} \quad (5.35)$$

Portanto, conforme as equações (5.34) e (5.35), a superposição entre os estados pode ser controlada através do valor do ângulo de fase ou polarização.

O principal problema é determinar a probabilidade mínima de erro P_e^E que um espião pode alcançar na determinação do bit. Nenhum tipo de restrição é imposto aos dispositivos físicos disponíveis para Eva, incluindo detectores perfeitos e capacidade computacional ilimitada.

O POVM ótimo para distinguir entre dois estados ρ_0 e ρ_1 é dado pelo processo de discriminação binária de Helstrom aplicado a $\Delta\rho = \rho_1 - \rho_0$ [42,44]. Denotando os projetores Π_1 e Π_0 ($\Pi_1 + \Pi_0 = I$) sobre auto-estados com autovalores positivos e negativos de $\Delta\rho$, a probabilidade de erro para Eva é dada por [42]

$$P_e^E = \text{Tr} [p_1 \Pi_0 \rho_1 + p_0 \Pi_1 \rho_0], \quad (5.36)$$

em que p_1 e p_2 são as probabilidades *a-priori* de encontrar um estado em ρ_1 e ρ_0 , respectivamente. Considerando $p_1 = p_2 = 1/2$, teremos [42]

$$P_e^E = \frac{1}{2} \text{Tr}[\Pi_0 \rho_1 + \Pi_1 \rho_0] = \frac{1}{2} (1 - \text{Tr}[\Pi_1 \Delta\rho]) = \frac{1}{2} \left(1 - 2 \sum_j \lambda_j \right), \quad (5.37)$$

em que λ_j são os autovalores positivos obtidos de [42]:

$$\Delta\rho = \frac{1}{M} \sum_{\nu=0}^{M-1} U_{\phi_\nu} (|\Psi_1\rangle\langle\Psi_1| - |\Psi_0\rangle\langle\Psi_0|) U_{\phi_\nu}^{-1}. \quad (5.38)$$

Com base no exposto acima, demonstra-se que a probabilidade mínima de erro de Eva $P_e^E \rightarrow 1/2$, para um número médio de fótons $|\alpha|^2$ pré-fixado, pode ser alcançada aumentando, prudentemente, o número de bases M . Desse modo, o sistema não possibilita detecção de presença de intrusos, mas garante que Eva não pode obter os bits enviados por Alice com total precisão. Por outro lado, Bob sabendo da chave usada por Alice na codificação, tem mais informação completa sobre o estado de luz enviado e pode extrair a informação com melhor precisão. Sua probabilidade de erro é [41]:

$$P_e^B = \frac{1}{2} \left(1 - \sqrt{1 - e^{-2|\alpha|^2}} \right). \quad (5.39)$$

Dessa forma, para um valor de α suficientemente grande, P_e^B é desprezível, levando a uma excelente recuperação do sinal por Bob.

Capítulo 6

CORREÇÃO DE ERRO QUÂNTICO APLICADA A ESTADOS COERENTES MESOSCÓPICOS COM ÓPTICA LINEAR

Para que o uso das tecnologias quânticas seja feito de forma eficiente e confiável, é necessário o emprego de sistemas de correção de erros. No caso dos sistemas de comunicação quântica que utilizam a polarização da luz, as maiores fontes de erro são a despolarização e as variações aleatórias da polarização devido às flutuações aleatórias da birrefringência da fibra ao longo de seu comprimento e do tempo. Para este último caso, sistemas de correção de erro baseados na transformação do qubit de polarização para qubit do tipo time-bin foram propostas [45-47]. Neste capítulo é mostrado como utilizar tais esquemas de correção de erro nos sistemas de comunicação quântica que usam estados coerentes mesoscópicos.

6.1 Sistema Ativo de Correção de Erro Quântico Aplicado a Estados Coerentes Mesoscópicos com Óptica Linear.

Nessa seção, é proposta a aplicação de um esquema óptico ativo, proposto em [45], para correção de erro do protocolo descrito na Seção 5.3. Considere o esquema óptico mostrado na Figura 6.1.

O rotacionador de polarização é passível de atuação direta de um sistema que o controle e, através dele, é impresso ao estado coerente $|\Psi\rangle = |\alpha, 0\rangle_{HV}$ o ângulo θ_A conforme o protocolo. A transformação unitária de um rotacionador de θ_A é dada por

$$R(\theta_A) = \begin{bmatrix} \cos \theta_A & -\sin \theta_A \\ \sin \theta_A & \cos \theta_A \end{bmatrix}. \quad (6.1)$$

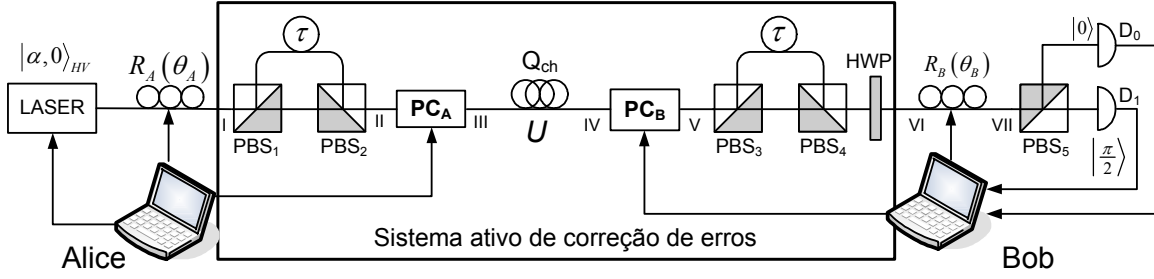


Figura 6.1: Sistema de comunicação quântica usando estados coerentes mesoscópicos e esquema ativo de correção de erro. PC - célula de Pockels.

Assim sendo, após passar pelo rotacionador o estado na saída é

$$|\Psi\rangle_I = |\alpha \cos \theta_A, \alpha \sin \theta_A\rangle. \quad (6.2)$$

Ao chegar ao chegar no PBS_1 os modos horizontal e vertical do estado coerente são separados, sendo que o horizontal percorre o braço inferior mais curto e o vertical percorre o braço superior mais longo que tem uma linha de atraso. Assim, os dois estão separados espacialmente e temporalmente. O estado após o PBS_2 de Alice é

$$|\Psi\rangle_{II} = |\alpha \cos \theta_A, 0\rangle_S \otimes |0, \alpha \sin \theta_A\rangle_L, \quad (6.3)$$

em que os índices S e L representam o caminho percorrido por cada modo como sendo curto e longo, respectivamente. A célula de Pockels PC_A atua apenas no estado atrasado (o que percorreu o braço longo) e rotaciona sua polarização em $\pi/2$. Assim, o estado lançado no canal de fibra óptica tem a forma

$$|\Psi\rangle_{III} = |\alpha \cos \theta_A, 0\rangle_S \otimes |\alpha \sin \theta_A, 0\rangle_L. \quad (6.4)$$

Considerando que a atuação do canal na polarização é expressa pela transformação unitária U , tal que

$$U|H\rangle = e^{i\phi} \cos \lambda |H\rangle + e^{i\chi} \sin \lambda |V\rangle \quad (6.5)$$

$$U|V\rangle = -e^{i\chi} \sin \lambda |H\rangle + e^{-i\phi} \cos \lambda |V\rangle, \quad (6.6)$$

o estado na entrada do aparato de Bob é

$$|\Psi\rangle_{IV} = \left| \alpha \cos \theta_A e^{i\phi} \cos \lambda, \alpha \cos \theta_A e^{i\chi} \sin \lambda \right\rangle_S \otimes \left| \alpha \sin \theta_A e^{i\phi} \cos \lambda, \alpha \sin \theta_A e^{i\chi} \sin \lambda \right\rangle_L. \quad (6.7)$$

Em Bob, a célula de Pockels PC_B atua agora no primeiro pulso (o que percorreu o braço curto em Alice), aplicando-lhe uma rotação de $\pi/2$, resultando em

$$|\Psi\rangle_V = \left| \alpha \cos \theta_A e^{i\chi} \sin \lambda, \alpha \cos \theta_A e^{i\phi} \cos \lambda \right\rangle_S \otimes \left| \alpha \sin \theta_A e^{i\phi} \cos \lambda, \alpha \sin \theta_A e^{i\chi} \sin \lambda \right\rangle_L. \quad (6.8)$$

No PBS_3 as componentes de cada um dos estados são novamente separadas, sendo que os modos horizontais do estado da equação anterior percorrem o braço inferior mais curto e os verticais percorrem o mais longo que possui uma nova linha de atraso. Portanto, o estado resultante após o PBS_4 e ao sofrer a ação do HWP é

$$|\Psi\rangle_{VI} = \left| 0, \alpha \cos \theta_A e^{i\chi} \sin \lambda \right\rangle_{SS} \otimes \left| \alpha \cos \theta_A e^{i\phi} \cos \lambda, \alpha \sin \theta_A e^{i\phi} \cos \lambda \right\rangle_{SL} \otimes \left| \alpha \sin \theta_A e^{i\chi} \sin \lambda, 0 \right\rangle_{LL}. \quad (6.9)$$

Finalmente, Bob aplica ao estado da equação (6.9) uma rotação de polarização θ_B conforme o protocolo. O estado resultante na entrada PBS_5 é

$$|\Psi\rangle_{VII} = \left| -\alpha \cos \theta_A \sin \theta_B e^{i\chi} \sin \lambda, \alpha \cos \theta_A \cos \theta_B e^{i\chi} \sin \lambda \right\rangle_{SS} \otimes \left| \alpha e^{i\phi} \cos \lambda \cos(\theta_A + \theta_B), \alpha e^{i\phi} \cos \lambda \sin(\theta_A + \theta_B) \right\rangle_{SL} \otimes \left| \alpha \sin \theta_A \cos \theta_B e^{i\chi} \sin \lambda, \alpha \sin \theta_A \sin \theta_B e^{i\chi} \sin \lambda \right\rangle_{LL}. \quad (6.10)$$

A rotação total realizada por Alice é $\theta_A = \theta_{bit} + \theta_{base}$, em que $\theta_{bit} = 0$ ou $\pi/2$. Por conhecer a seqüência das bases usadas por Alice na modulação, a rotação aplicada por Bob também é $\theta_B = -\theta_{base}$. Sendo assim, as rotações aplicadas por cada um devem ser tais que a condição $\theta_A + \theta_B = \theta_{bit}$ seja obtida. Com base no exposto e na equação (6.10), temos que, se $\theta_{bit} = 0$, o estado resultante na entrada do PBS_5 é

$$|\Phi\rangle_{VII}^0 = \left| \alpha \frac{\sin(2\theta_{Base})}{2} e^{i\chi} \sin \lambda, \alpha \cos^2 \theta_{Base} e^{i\chi} \sin \lambda \right\rangle_{SS} \otimes \left| \alpha \cos \lambda e^{i\phi}, 0 \right\rangle_{SL} \otimes \left| \alpha \frac{\sin(2\theta_{Base})}{2} e^{i\chi} \sin \lambda, -\alpha \sin^2 \theta_{base} \sin \lambda e^{i\chi} \right\rangle_{LL}, \quad (6.11)$$

e se $\theta_{bit} = \pi/2$,

$$|\Phi\rangle_{VII}^{\pi/2} = \left| -\alpha \sin^2 \theta_{base} e^{i\chi} \sin \lambda, -\alpha \frac{\sin(2\theta_{base})}{2} e^{i\chi} \sin \lambda \right\rangle_{SS} \otimes \left| 0, \alpha \cos \lambda e^{i\phi} \right\rangle_{SL} \otimes \left| \alpha \cos^2 \theta_{base} e^{i\chi} \sin \lambda, -\alpha \frac{\sin(2\theta_{base})}{2} e^{i\chi} \sin \lambda \right\rangle_{LL}. \quad (6.12)$$

Portanto, observando (6.11) e (6.12), pode-se notar que o estado intermediário SL contém a informação ou bit que Alice deseja transmitir para Bob com valor proporcional a $\cos \lambda$.

6.2 Sistema Passivo de Correção de Erro Quântico Aplicado a Estados Coerentes Mesoscópicos com Óptica Linear.

O sistema óptico de correção de erros apresentado na Figura 6.1, utilizando células de Pockels, também funciona corretamente quando fótons isolados são utilizados [45]. Entretanto, quando da utilização de estados coerentes, sistemas ópticos passivos de correção de erros podem ser implementados, eliminando a árdua tarefa de sincronização das células de Pockels. O preço a ser pago, como será mostrado, é uma perda da potência óptica útil. O sistema óptico para correção passiva de erros proposto em [47] está ilustrado na Figura 6.2.

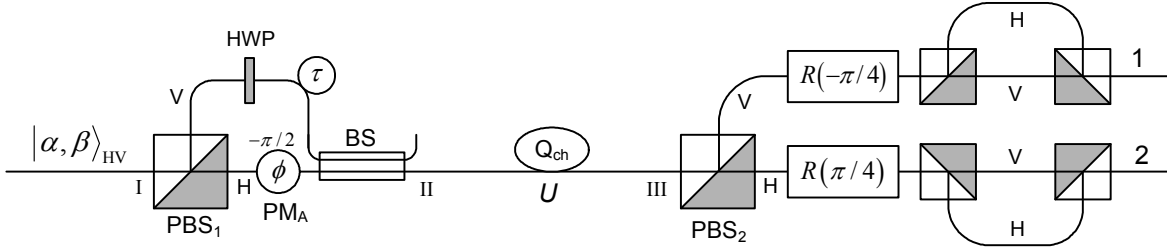


Figura 6.2: Esquema passivo para correção de erros. BS – Acoplador óptico balanceado.

Na Figura 6.2 BS é um acoplador óptico balanceado com transmitância $T = 1/\sqrt{2}$ e refletância $R = i/\sqrt{2}$. O estado quântico de entrada é $|\alpha, \beta\rangle$ e o sistema funciona como segue: as componentes do estado inicial são separadas pelo primeiro PBS. A componente horizontal percorre o caminho curto (S), recebendo a fase $-\pi/2$, enquanto a componente vertical percorre o caminho longo (τ), passando através de uma HWP (placa de meia onda), resultando em $|-i\alpha, 0\rangle_S \otimes |\beta, 0\rangle_L$. Após a passagem por BS, ambos os pulsos são lançados no canal quântico, separados pelo intervalo de tempo entre o pulso curto e o pulso longo. O estado de entrada no canal é $|\alpha/\sqrt{2}, 0\rangle_S \otimes |\beta/\sqrt{2}, 0\rangle_L$. O estado na saída do canal modelado por (6.5)-(6.6) é:

$$\left| \frac{\alpha}{\sqrt{2}} \cos(\varphi) e^{i\lambda}, \frac{\alpha}{\sqrt{2}} \sin(\varphi) e^{i\xi} \right\rangle_S \otimes \left| \frac{\beta}{\sqrt{2}} \cos(\varphi) e^{i\lambda}, \frac{\beta}{\sqrt{2}} \sin(\varphi) e^{i\xi} \right\rangle_L. \quad (6.13)$$

Em (6.13) φ , λ e ξ são parâmetros de uma transformação unitária geral. As componentes de (6.13) são separadas pelo PBS₂ em Bob, resultando no seguinte estado total:

$$\left| \frac{\alpha}{\sqrt{2}} \cos(\varphi) e^{i\lambda}, 0 \right\rangle_S^2 \otimes \left| 0, \frac{\alpha}{\sqrt{2}} \sin(\varphi) e^{i\xi} \right\rangle_S^1 \otimes \left| \frac{\beta}{\sqrt{2}} \cos(\varphi) e^{i\lambda}, 0 \right\rangle_L^2 \otimes \left| 0, \frac{\beta}{\sqrt{2}} \sin(\varphi) e^{i\xi} \right\rangle_L^1. \quad (6.14)$$

As componentes verticais viajam pelo caminho 1 e as componentes horizontais viajam pelo caminho 2. No caminho 1 há um rotacionador de polarização de ângulo $-\pi/4$, $R(-\pi/4)$. Após este rotacionador, o estado no caminho 1 é:

$$\left| \frac{\alpha}{2} \sin(\varphi) e^{i\xi}, \frac{\alpha}{2} \sin(\varphi) e^{i\xi} \right\rangle_S^1 \otimes \left| \frac{\beta}{2} \sin(\varphi) e^{i\xi}, \frac{\beta}{2} \sin(\varphi) e^{i\xi} \right\rangle_L^1. \quad (6.15)$$

Por fim, logo após o rotacionador há um interferômetro de polarização em que a componente vertical toma o caminho curto S enquanto que a componente horizontal toma o caminho longo L . Assim, o estado final na saída do percurso 1 é:

$$\left| 0, \frac{\alpha}{2} \sin(\varphi) e^{i\xi} \right\rangle_{SS}^1 \otimes \left| \frac{\alpha}{2} \sin(\varphi) e^{i\xi}, \frac{\beta}{2} \sin(\varphi) e^{i\xi} \right\rangle_{SL}^1 \otimes \left| \frac{\beta}{2} \sin(\varphi) e^{i\xi}, 0 \right\rangle_{LL}^1. \quad (6.16)$$

Semelhantemente, após passar pelo rotacionador $R(\pi/4)$ e pelo interferômetro de polarização, o estado na saída do percurso 2 é:

$$\left| 0, \frac{\alpha}{2} \cos(\varphi) e^{i\lambda} \right\rangle_{SS}^2 \otimes \left| \frac{\alpha}{2} \cos(\varphi) e^{i\lambda}, \frac{\beta}{2} \cos(\varphi) e^{i\lambda} \right\rangle_{SL}^2 \otimes \left| \frac{\beta}{2} \cos(\varphi) e^{i\lambda}, 0 \right\rangle_{LL}^2. \quad (6.17)$$

Como pode ser observado em (6.16) e (6.17), em cada saída haverá três pulsos, sendo que o pulso no tempo central, LS , possui a mesma polarização do pulso enviado no transmissor. Percebemos ainda que 1/4 da energia do pulso de entrada corresponde à energia do pulso corrigido na saída para o caso de uma fibra sem perdas.

Percebe-se que o esquema de correção mostrado na Figura 6.2 é passivo, pois não necessita da atuação de células de Pockels. Por outro lado, Bob deve levar em consideração apenas os pulsos no tempo intermediário LS .

A utilização do esquema passivo de correção de erro descrito, em um sistema de comunicação quântica usando estados coerentes mesoscópicos, é mostrada na Figura 6.3 [48].

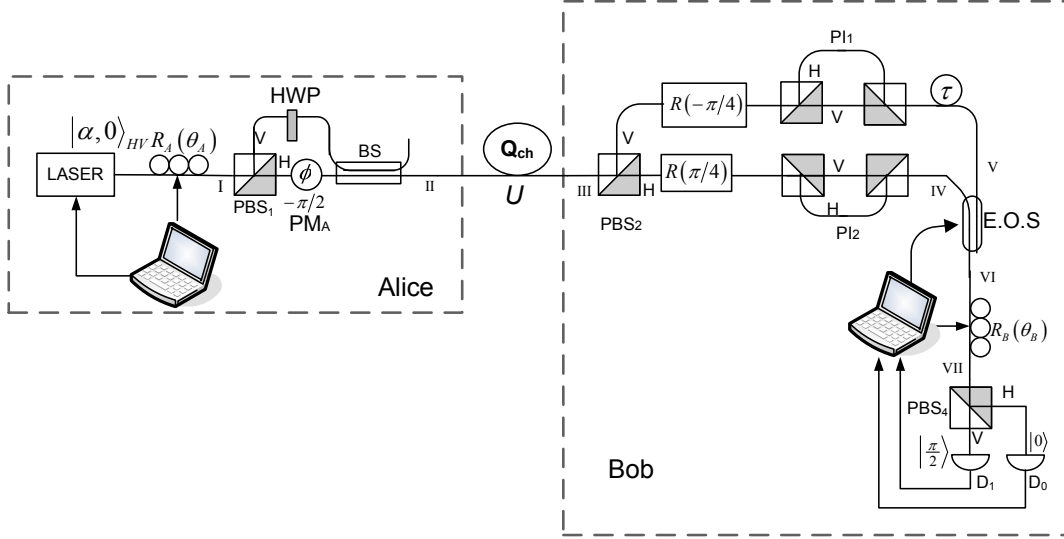


Figura 6.3: Sistema de comunicação quântica usando estados coerentes mesoscópicos e esquema passivo de correção de erro. E.O.S – chave eletro-ótica.

O estado gerado por Alice é:

$$R(\theta_A)|\alpha, 0\rangle = \exp\left(-\theta_A(\hat{a}_V^+\hat{a}_H - \hat{a}_H^+\hat{a}_V)\right)|\alpha, 0\rangle = |\alpha \cos(\theta_A), \alpha \sin(\theta_A)\rangle, \quad (6.18)$$

sendo \hat{a}_V e \hat{a}_H são, respectivamente, os operadores aniquilação dos modos vertical e horizontal. O protocolo de comunicação é o usual: Alice escolhe dois ângulos de polarização: $\phi_a^{bit} \in \{0, \pi/2\}$ para o bit, e $\phi_a^{base} \in \{1, \dots, M\}$ onde M , um inteiro ímpar, é o número de bases. Portanto, o estado quântico do pulso enviado por Alice é aquele dado em (6.18) tendo $\theta_A = \phi_a^{bit} + \phi_a^{base}$. Após a propagação no canal óptico com o esquema passivo corretor de erros, o estado que chega no rotacionador de polarização de Bob no tempo $LS + \tau$ (τ é um atraso devido a um enlace extra de fibra no caminho 1) e LS (os pulsos nos tempos SS e LL não serão considerados) são, respectivamente:

$$|\Psi_f^1\rangle = \left| \frac{\alpha \cos(\theta_A)}{2} \sin(\varphi) e^{i\xi}, \frac{\alpha \sin(\theta_A)}{2} \sin(\varphi) e^{i\xi} \right\rangle_{SL}^1 \quad (6.19)$$

$$|\Psi_f^2\rangle = \left| \frac{\alpha \cos(\theta_A)}{2} \cos(\varphi) e^{i\lambda}, \frac{\alpha \sin(\theta_A)}{2} \cos(\varphi) e^{i\lambda} \right\rangle_{SL}^2 \quad (6.20)$$

Após a ação de Bob referente ao protocolo, os estados são:

$$|\Psi_f^1\rangle = \left| \frac{\sin(\varphi)e^{i\xi}}{2} \alpha \cos(\theta_A + \theta_B), \frac{\sin(\varphi)e^{i\xi}}{2} \alpha \sin(\theta_A + \theta_B) \right\rangle_{SL}^1 \quad (6.21)$$

$$|\Psi_f^2\rangle = \left| \frac{\cos(\varphi)e^{i\lambda}}{2} \alpha \cos(\theta_A + \theta_B), \frac{\cos(\varphi)e^{i\lambda}}{2} \alpha \sin(\theta_A + \theta_B) \right\rangle_{SL}^2. \quad (6.22)$$

Os valores escolhido por Bob para θ_B são aqueles previamente acordados com Alice, $\theta_B = -\phi_A^{base}$, como requerido pelo protocolo de comunicação quântica utilizando estados coerentes mesoscópicos. Portanto, os estados que chegam ao medidor de Bob (último PBS + fotodetectores) são:

$$|\Psi_f^1\rangle = \left| \frac{\sin(\varphi)e^{i\xi}}{2} \alpha \cos(\phi_A^{bit}), \frac{\sin(\varphi)e^{i\xi}}{2} \alpha \sin(\phi_A^{bit}) \right\rangle_{SL}^1 = \begin{cases} |0.5 \sin(\varphi)e^{i\xi} \alpha, 0\rangle & \text{if } \phi_A^{bit} = 0 \\ |0, 0.5 \sin(\varphi)e^{i\xi} \alpha\rangle & \text{if } \phi_A^{bit} = \frac{\pi}{2} \end{cases} \quad (6.23)$$

$$|\Psi_f^2\rangle = \left| \frac{\cos(\varphi)e^{i\lambda}}{2} \alpha \cos(\phi_A^{bit}), \frac{\cos(\varphi)e^{i\lambda}}{2} \alpha \sin(\phi_A^{bit}) \right\rangle_{SL}^2 = \begin{cases} |0.5 \cos(\varphi)e^{i\lambda} \alpha, 0\rangle & \text{if } \phi_A^{bit} = 0 \\ |0, 0.5 \cos(\varphi)e^{i\lambda} \alpha\rangle & \text{if } \phi_A^{bit} = \frac{\pi}{2} \end{cases} \quad (6.24)$$

Portanto, o bit medido por Bob é o mesmo enviado por Alice. Como pode ser visto em (6.19)-(6.24), o esquema corretor de erro faz com que Bob receba duas cópias do estado enviado por Alice.

Capítulo 7

SISTEMAS HÍBRIDOS DE DISTRIBUIÇÃO QUÂNTICA DE CHAVES

A segurança incondicional dos sistemas de comunicação quântica que usam estados coerentes mesoscópicos mostrados no Capítulo 5 ainda é questão de intensos debates [49-54]. É possível que tais sistemas sejam incondicionalmente seguros para uso em encriptação direta, isto é, no sentido real da frase “criptografia quântica”. Assim, Alice pode enviar uma mensagem (sem criptografia algorítmica) para Bob encriptada nos estados coerentes mesoscópicos (criptografia física). Por outro lado, parece ser consenso que os sistemas do Capítulo 5 não são incondicionalmente seguros para distribuição quântica de chaves, isto é, uma mensagem enviada por Alice para Bob usando o sistema que usa estados coerentes mesoscópicos do Capítulo 5, não pode ser diretamente utilizada como chave. Isto ocorre devido ao uso de um gerador de números pseudo-aleatório para a expansão da chave inicialmente dividida por Alice e Bob. Entretanto, foi recentemente proposto que é possível realizar distribuição quântica de chaves fazendo uso conjunto de estados coerentes mesoscópicos e fortemente atenuados [55,56]. Uma possível implementação óptica deste sistema híbrido é proposta neste capítulo, bem como a análise da segurança contra o ataque de força bruta.

7.1 Distinção de Estados Coerentes Polarizados: Número Médio de Fótons Versus Número de Bases.

Suponhamos que um transmissor envia ao receptor um estado coerente linearmente polarizado, escolhido de forma equiprovável no conjunto $\{|\theta_0\rangle, \dots, |\theta_{M-1}\rangle\}$, $0 \leq \theta \leq \pi/2$. O objetivo do receptor é identificar a polarização, e portanto, a seqüência de bits enviada. Se o pulso contém muitos fótons, o receptor poderá aplicar a estratégia da força bruta, ou seja, ele divide o pulso que recebe em M outros pulsos com a mesma polarização. Para o pulso P_i

o receptor aplica uma rotação na polarização de $-\theta_i$ e passa o pulso por um PBS que possui um detector em cada saída. O esquema é mostrado na Figura 7.1.

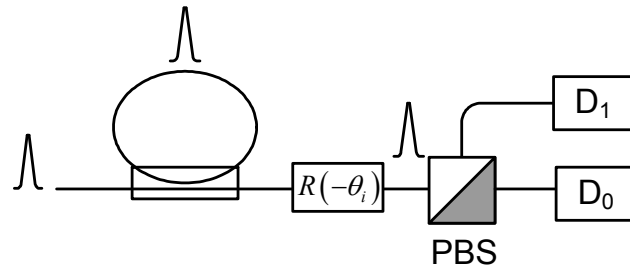


Figura 7.1: Medição da polarização de um pulso coerente multifótons usando a força bruta.

Se o receptor possui detectores perfeitos (eficiência unitária e sem ruído), então os seguintes casos são possíveis:

- 1) Detecção em ambos os detectores. Neste caso o receptor sabe que a rotação de polarização aplicada está errada.
- 2) Nenhuma detecção. Neste o receptor não ganha nenhuma informação.
- 3) Detecção em apenas um dos detectores. Neste caso há duas possibilidades:
 - 3.1) A rotação de polarização aplicada está correta.
 - 3.2) A rotação de polarização está errada, mas um dos modos nas saídas do PBS tem zero fóton.

Portanto, se o pulso óptico enviado pelo transmissor tem um número de fótons muito maior que o número de palavras do código utilizado, isto é, maior que M , então com alta probabilidade o receptor conseguirá determinar a polarização enviada. Por outro lado, se o número de fótons do pulso é muito menor que M , então o receptor não terá fótons suficientes para testar todas as possíveis rotações de polarização e não será capaz de determinar com boa precisão a polarização enviada. Quanto menor for a separação entre os estados de polarização, maior M e maior deverá ser o número médio de fótons do estado coerente para que o receptor consiga uma boa relação sinal ruído em sua medição. É possível que, se $|\alpha|^2 \ll M$, o receptor utilize um amplificador óptico de forma a aumentar o número de fótons. Entretanto, o processo de amplificação implica na produção de fótons

totalmente despolarizados, emitidos por emissão espontânea. Este efeito, que é inevitável, pois é exatamente ele que proíbe que amplificadores ópticos sejam usados para clonar a polarização de um fóton, limita o benefício que a amplificação pode proporcionar na relação sinal-ruído.

7.2 Sistema de Distribuição Quântica de Chaves Híbrido

O protocolo de DQC empregando estados coerentes fracos e mesoscópicos possui as seguintes etapas:

1. Alice e Bob dividem antecipadamente uma chave de K bits. Usando esta chave como semente em um gerador de números aleatórios, a chave é expandida para outra de K' bits.
2. Alice gera uma seqüência aleatória de bits. Cada bit é encriptado na polarização de um estado coerente mesoscópico, como explicado no Capítulo 5, e enviado para Bob.
3. A seqüência gerada por Alice e enviada para Bob é utilizada por ambos para a escolha da base do protocolo BB84 utilizando estados coerentes fracos.
4. O protocolo BB84 é executado sendo que, como explicado no Tópico 3, a escolha aleatória das bases é substituída pela escolha segundo os bits gerados por Alice e enviados em estados coerentes mesoscópicos para Bob.

As vantagens são:

1. Nenhum bit é perdido, uma vez que Alice e Bob escolhem a mesma base sempre. Isto obviamente dobra a taxa de transmissão de bits úteis.
2. Ao final do protocolo Alice e Bob não divulgarão as bases utilizadas, o que torna inútil a utilização de memória quântica por parte de Eva.

A espiã tentará interceptar os pulsos mesoscópicos enviado por Alice e determinar a polarização. Tendo sucesso, ela saberá a base a ser utilizada e poderá fazer uma medição sem erros do qubit enviado por Alice. Entretanto, como mostrado na Seção 7.1, Eva não conseguirá realizar esta tarefa com perfeição se o número de bases de polarização sendo utilizado for muito maior que o número médio de fótons dos pulsos enviados por Alice.

Além disso, Bob pode monitorar a potência dos pulsos mesoscópicos e a taxa de erro em suas medições para avaliar se Eva utilizou um amplificador óptico. Se Eva utilizar o amplificador óptico, fótons despolarizados alcançarão o detector de Bob e poderão causar detecções onde não deveriam ocorrer uma vez que Bob, por conhecer a chave K' , sabe exatamente como recuperar apenas o bit que Alice enviou. Um exemplo de implementação do sistema híbrido é mostrado na Figura 7.2. Como pode ser visto nela, o canal de 1300nm é utilizado para a comunicação quântica com estados mesoscópicos empregando correção de erro enquanto que o canal de 850nm suporta o protocolo BB84 polarimétrico.

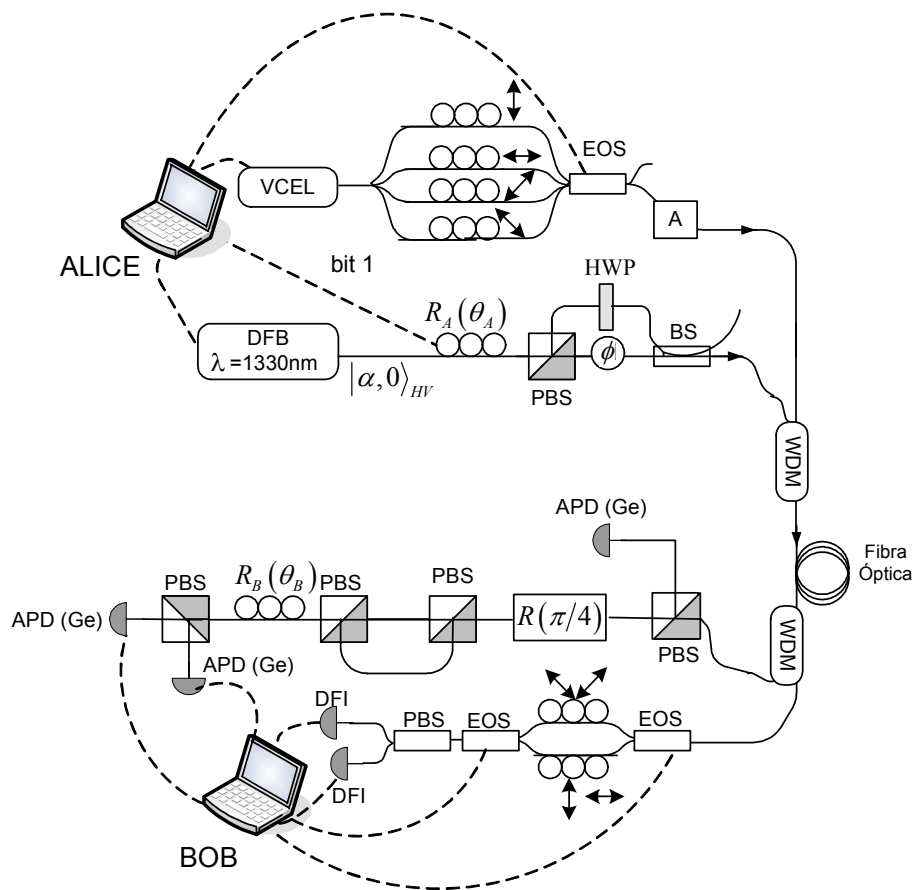


Figura 7.2: Sistema de DQC híbrido que executa o protocolo BB84 polarimétrico.

7.3 Sistema de Híbrido de Autenticação Quântica de Mensagens Clássicas

Um protocolo de autenticação quântica de mensagens clássicas foi proposto em [57]. O digrama em blocos do protocolo é mostrado na Figura 7.3.

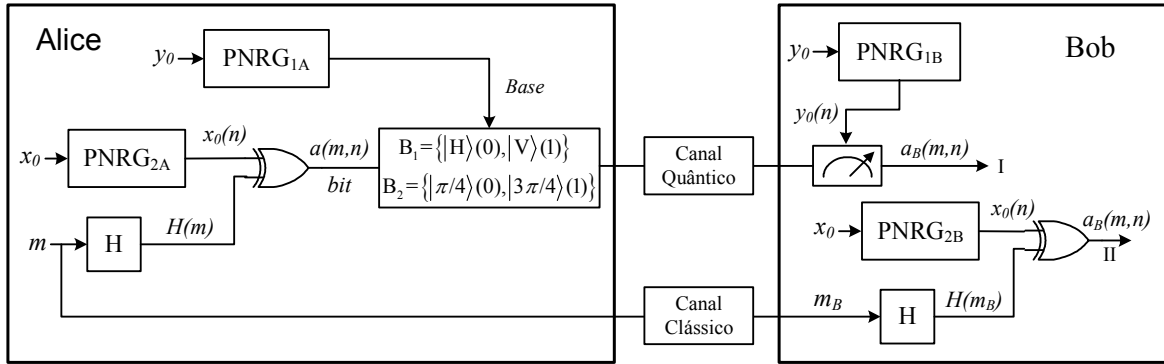


Figura 7.3: Protocolo de autenticação quântica de mensagens clássicas.

O protocolo funciona da seguinte maneira: Alice e Bob dividem antecipadamente duas sementes, x_0 e y_0 . Cada uma delas é passada por um gerador de números pseudo-aleatório que pode ser do tipo Blum-Micali ou Blum-Blum-Shub. Por outro lado, Alice tem uma mensagem m e vai transmiti-la para Bob. Este quer ter certeza que a mensagem partiu de Alice. Alice calcula a função hash de m , $H(m)$, e a esconde fazendo a operação xor da mesma com a seqüência de bits gerada por PNRG_{2A} . O resultado desta operação é $a(m,n)$. Agora, Alice usa os bits da seqüência gerada por PNRG_{1A} , cuja semente é y_0 , para escolher uma base, B_1 ou B_2 , e os bits de $a(m,n)$ para escolher o estado da base, exatamente como ocorre no protocolo BB84. Estes qubits são então enviados para Bob. Este, por sua vez, usa a seqüência de bits gerada por PNRG_{1B} , cuja semente é y_0 , para medir os qubits enviados por Alice na base correta, obtendo $a_B(m,n)$ na saída I. Por outro lado, ao receber a mensagem m_B Bob calcula a função hash da mesma, $H(m_B)$, e a função xor de $H(m_B)$ com os bits gerados por PNRG_{2B} cuja semente é x_0 , cujo resultado é $a_B(m,n)$ na saída II. Se a mensagem m_B for realmente a enviada por Alice, então as duas saídas I e II são iguais.

A aplicação do sistema híbrido na implementação do protocolo de autenticação quântica de mensagens clássicas é direta. Como no caso da distribuição quântica de chaves, Alice usa estados coerentes mesoscópicos para enviar para Bob a informação sobre qual base ele deve utilizar. O mesmo esquema da Figura 7.2 pode ser utilizado.

Capítulo 8

RECEPTOR ÓPTICO PARA INSTRUMENTAÇÃO E COMUNICAÇÃO

O receptor óptico é um importante instrumento em laboratórios de comunicação óptica, onde geralmente é usado, por exemplo, como medidor de potência óptica ou conversor em experimentos ópticos, para recuperação da informação impressa na potência óptica através da conversão em variações de sinais elétricos (capaz de ser tratado por um computador, por exemplo) [58]. Os componentes ópticos responsáveis por converter sinais ópticos em sinais elétricos são os fotodiodos PIN e APD. No circuito usado para amplificação do sinal é usado um amplificador de banda larga. Neste estágio, o ruído aparece devido às fontes de ruído intrínsecos do amplificador, o ruído térmico dos resistores e do ruído *shot* do fotodiodo. Além do amplificador, são usados no circuito componentes lógicos da família PECL que oferecem melhor resposta e rapidez a variações velozes de um pulso óptico curto [58].

8.1 Análise Teórica

O circuito eletrônico de um receptor óptico é usualmente constituído por um fotodiodo, PIN ou APD, seguido de um amplificador operacional rápido de banda larga como mostrado na Figura 8.1.

O circuito integrado CLC449 é um amplificador operacional de alta velocidade, de -3dB e largura de banda -3dB de 1,2GHz com ganho de +2. Quando usado na configuração não inversora de ganho variável, como mostrado no esquema da Figura 8.1, ele amplifica a tensão através do segundo resistor de 1kΩ. Tal circuito pode operar em sistemas ópticos analógicos que empregam taxas de modulação da ordem de 1GHz ou em sistemas ópticos digitais detectando pulsos ópticos com larguras da ordem de 10^{-9} s.

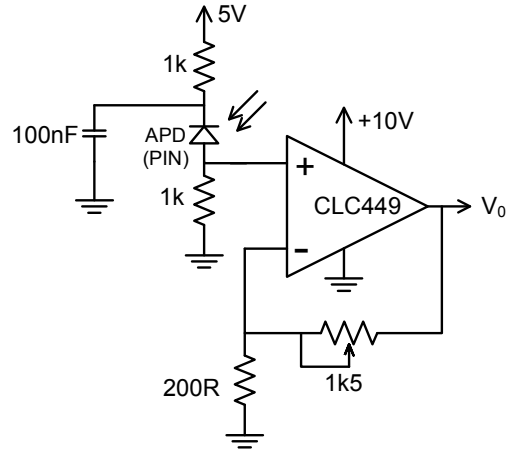


Figura 8.1: Circuito eletrônico do receptor óptico.

A fim de analisar o processamento do sinal realizado pelo receptor óptico proposto, é usado o modelo de sinal AC mostrado na Figura 8.2.

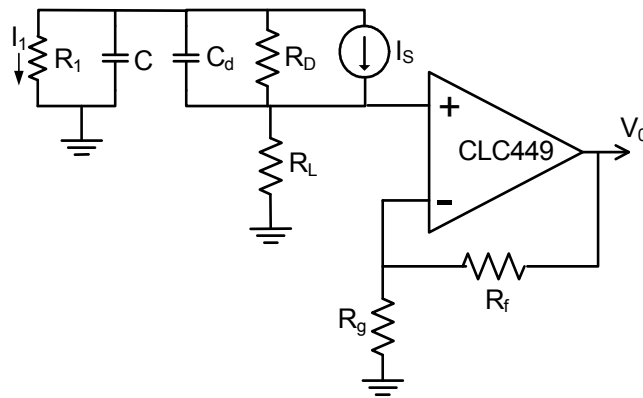


Figura 8.2: Modelo AC para o receptor óptico.

No modelo, o fotodiodo é substituído por sua resistência interna R_d e capacitância C_d . O sinal, I_s , é a fotocorrente através do componente que é dada por [58]

$$I_s = M \mathfrak{R}_0 P_i \quad (\text{APD}) \quad (8.1)$$

$$I_s = \mathfrak{R}_0 P_i \quad (\text{PIN}), \quad (8.2)$$

em que P_i é a potência óptica incidente do fotodetector. M é o fator multiplicativo de corrente para o fotodiodo de avalanche que pode ser determinado pela expressão [58]

$$M = \frac{1}{1 - (V/V_B)^n}. \quad (8.3)$$

Em (4.3), V é a tensão reversa aplicada ao FDA, V_B é a tensão de ruptura, n é um parâmetro ajustável usado para adaptar o modelo teórico aos dados experimentais. \mathfrak{R}_0 é a responsividade dada por [58]

$$\mathfrak{R}_0 = \frac{\eta\lambda}{1.24}, \quad (8.4)$$

que é função do comprimento de onda λ , em μm , e da eficiência quântica η .

O conjunto de equações diferenciais que modela o circuito eletrônico mostrado na Figura 4.2 é [58]

$$R_1 C R_d C_d \frac{d^2 I_1}{dt^2} + \left[\frac{R_L R_1}{R_d} C + R_L C_d + R_1 (C + C_d) \right] \frac{dI_1}{dt} + \left(1 + \frac{R_L + R_1}{R_d} \right) I_1 = I_s \quad (8.5)$$

$$-R_L R_1 C \frac{dI_1}{dt} - R_L I_1 = V_i \quad (8.6)$$

$$V_o = A_v V_i = \left(1 + \frac{R_f}{R_g} \right) V_i. \quad (8.7)$$

Objetivando encontrar a solução do sistema (8.5)-(8.7) para diferentes formatos de I_s e P_i , conforme (8.1) e (8.2), podemos usar o método da série de Fourier. Suponhamos as seguintes expansões para I_s e I_1 :

$$I_s = \sum_{n=-\infty}^{+\infty} a_n e^{in\omega t}; \quad I_1 = \sum_{n=-\infty}^{+\infty} b_n e^{in\omega t}. \quad (8.8)$$

Substituindo (8.8) em (8.5) e (8.6), obtemos

$$b_n = \frac{a_n}{\frac{R_L + R_1 + R_d}{R_d} - n^2 \omega^2 R_1 C R_d C_d + in\omega \left[\frac{R_1 (R_L + R_d)}{R_d} C + (R_L + R_1) C_d \right]} \quad (8.9)$$

$$V_o = \left(1 + \frac{R_f}{R_g} \right) \sum_{n=-\infty}^{+\infty} -(R_L + in\omega R_L R_1 C) b_n e^{in\omega}, \quad (8.10)$$

em que os coeficientes a_n podem ser obtidos de $I_S(t)$ através da relação

$$a_n = \frac{\omega}{2\pi} \int_{-\pi/\omega}^{\pi/\omega} I_S(t) e^{-in\omega t} dt. \quad (8.11)$$

Por outro lado, quando queremos considerar o ruído que limita a sensibilidade do receptor, devemos usar o modelo *AC* para o ruído mostrado na Figura 8.3.

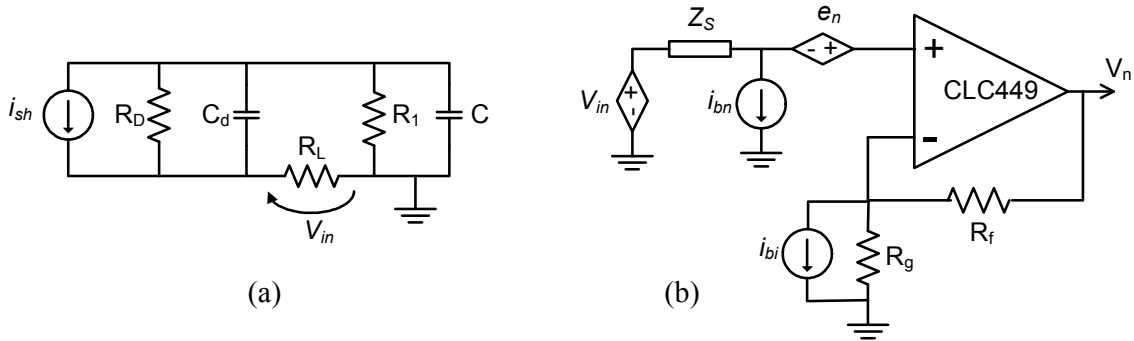


Figura 8.3: Modelo *AC* com ruído para o receptor óptico.

V_{in} é a tensão do ruído na entrada do amplificador e é função do ruído balístico (*shot*) do fotodiodo e do ruído térmico dos resistores do circuito da Figura 8.3.a. O ruído balístico é dado por [58]

$$\overline{i_{sh}^2} = 2e(I_s + I_d) \text{ (PIN)} \quad [A^2/Hz] \quad (8.12)$$

$$\overline{i_{sh}^2} = 2e(I_s + I_d) M^2 F \text{ (APD)} \quad [A^2/Hz], \quad (8.13)$$

em que F é o fator de ruído excedente usado para o FDA, que modela o ruído adicional produzido pelo processo de multiplicação de corrente de avalanche. Sendo assim, a Figura 8.3.a pode ser então modelada por uma fonte de tensão de ruído V_{in} e impedância Z_s dadas por [58]

$$Z_s = \frac{R_L (Z_d + Z_1)}{R_L + (Z_d + Z_1)} = R_0(\omega) + iS_0(\omega), \quad (8.14)$$

$$\bar{V}_{in}^2 = 4kTR_0 + \bar{i}_{sh}^2 \left| \frac{Z_d R_L}{R_L + Z_1 + Z_d} \right|^2 \quad [V^2/Hz], \quad (8.15)$$

$$Z_d = \frac{R_d}{1 + j\omega R_d C_d}; \quad Z_1 = \frac{R_1}{1 + j\omega R_1 C}. \quad (8.16)$$

Em (8.15), $4kT=16 \times 10^{-21} \text{J}$, para $T=290\text{K}$. Já na Figura 8.3.b, as fontes de ruído, conforme folha de dados do fabricante do CLC449, são e_n (com valor típico de $2\text{nV}/(\text{Hz})^{1/2}$ a 1MHz), i_{bi} (com valor típico de $15\text{pA}/(\text{Hz})^{1/2}$ a 1MHz) e i_{bn} (com valor típico de $3\text{pA}/(\text{Hz})^{1/2}$ a 1MHz). Portanto, a tensão de ruído na saída e a relação sinal-ruído são [58]

$$\bar{V}_n^2 = \left(1 + \frac{R_f}{R_g} \right) \left[\bar{i}_{bn}^2 |Z_s|^2 + \bar{V}_{in}^2 + \bar{e}_n^2 + i_{bi}^2 \left(\frac{R_g R_f}{R_g + R_f} \right)^2 + 4kT \left(\frac{R_g R_f}{R_g + R_f} \right) \right] \quad [V^2/Hz] \quad (8.17)$$

$$\text{SNR} = \int_{-\infty}^{+\infty} \bar{V}_o^2 |H(j\omega)|^2 d\omega / \int_{-\infty}^{+\infty} \bar{V}_n^2 |H(j\omega)|^2 d\omega, \quad (8.18)$$

em que $H(j\omega)$ é a função de transferência de tensão do amplificador.

8.2 Resultados Experimentais

O receptor óptico mostrado na Figura 8.1 foi construído no LATIQ e diversos testes foram realizados tendo como fonte de radiação o diodo laser CQF915/108 operando em modo contínuo (CW) em $1550,91\text{nm}$. Os parâmetros considerados para análise foram: a temperatura do laser de $1\text{k}\Omega$ até $10\text{k}\Omega$ (valores da resistência interna do termistor NTC do laser) e a corrente de injeção do laser, de 15mA até 43mA , sendo que a potência de saída é

função de ambos. A Figura 8.4 mostra o esquema usado em que a fonte do laser LDC205 e o controlador de temperatura TED 200 são da Thorlabs, e os fotodiodos usados foram: o PIN FGA04, da Thorlabs, e o APD C30645E, da Perkin Elmer, ambos de InGaAs.

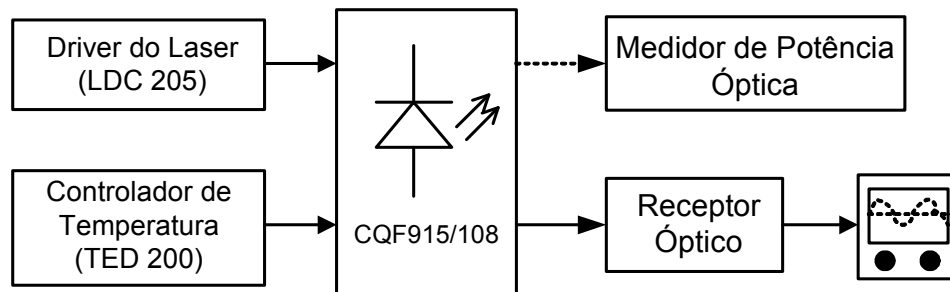


Figura 8.4: Esquema usado nos testes do receptor óptico.

A Figura 8.5 mostra a dependência da potência de saída versus corrente de injeção do laser para dois valores de temperatura.

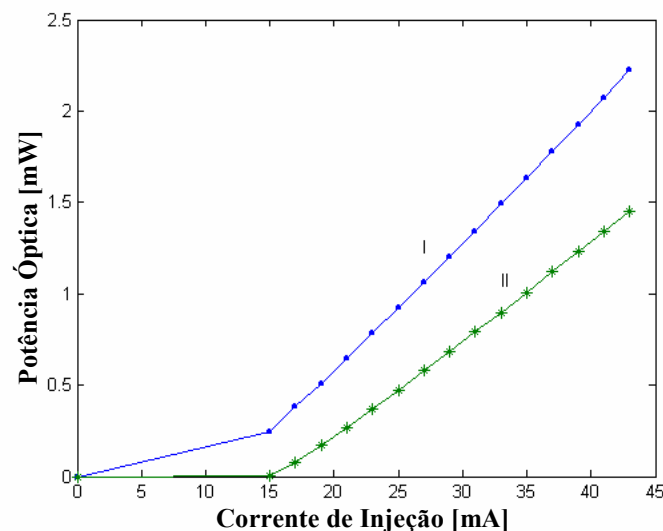


Figura 8.5: Potência de saída do laser [mW] versus corrente de injeção do laser [mA] para dois valores de temperaturas: (I) 10kΩ e (II) 5kΩ.

Podemos observar que a potência aumenta quando a temperatura diminui e a corrente aumenta. Além disso, da folha de dados do laser, a potência de saída para $T=9,2\text{k}\Omega$ e $I_L=43\text{mA}$ é 2,2mW, enquanto que foi obtido, para $T=10\text{k}\Omega$ e $I_L=43\text{mA}$, uma potência de 2,187mW.

Na Figura 8.6, observa-se a tensão de saída, V_o , na saída do amplificador CLC449 versus a potência óptica incidente, para $T=10k\Omega$, para ambos os fotodiodos. A relação entre a potência de entrada e a tensão de saída é mais linear para o fotodiodo PIN, principalmente para potências de entrada maiores que 1mW. É importante ressaltar que, devido à baixa tensão reversa aplicada ao FDA, $M\sim 1$ e ele opera semelhantemente como um PIN. A Figura 8.7 mostra a caracterização completa do PIN FGA04.

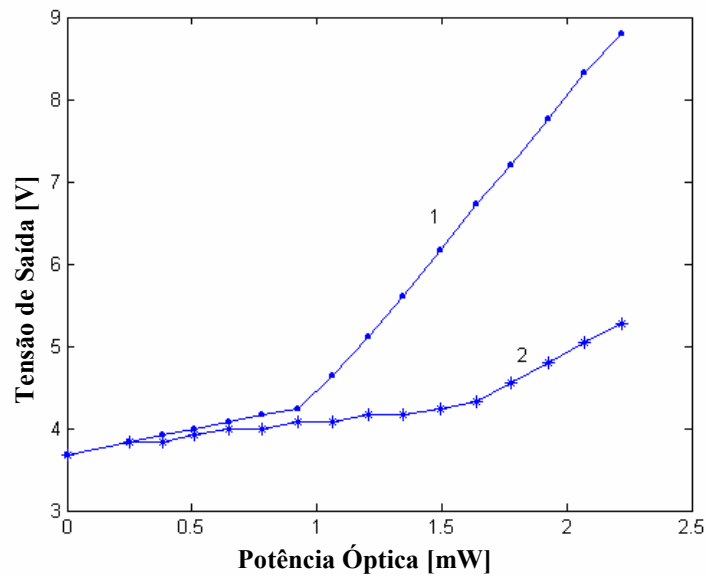


Figura 8.6: Tensão de saída do receptor óptico versus potência óptica incidente com laser operando na temperatura de 10k Ω : (1) PIN FGA04 e (2) FDA C30645E.

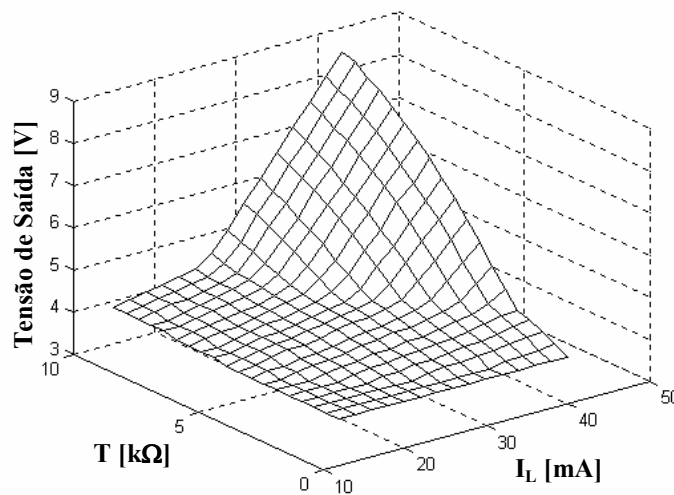


Figura 8.7: Tensão de saída do receptor óptico, V_o , versus a temperatura do laser e corrente de injeção, usando o fotodiodo PIN FGA04.

O formato da curva mostrado na Figura 8.7 é bastante semelhante ao que acontece com a potência do laser quando sua temperatura T e corrente de injeção I_L são variados. Portanto, com base nas Figuras 8.6 e 8.7, a relação entre potência óptica incidente e tensão de saída pode ser determinada e é dada por

$$V_o = GV_i = GR_L I_s = GR_L M \mathfrak{R}_0 P = \mathfrak{R}_e P. \quad (8.19)$$

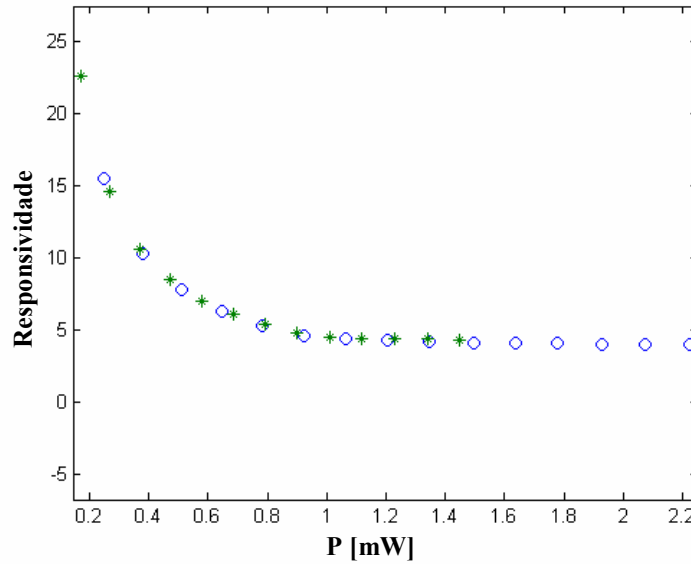


Figura 8.8: Resposta \mathfrak{R}_e [V/mW] versus potência de saída do laser para o fotodiodo FGA04 para as temperaturas $T_L=10\text{k}\Omega$ (o) e $T_L=5\text{k}\Omega$ (*).

A fim de calcular \mathfrak{R}_e para o fotodiodo FGA04, a curva V_o/P versus P , para temperaturas de $10\text{k}\Omega$ (o) e $5\text{k}\Omega$ (*) podem ser vistas na Figura 8.8.

O valor elevado da resposta para baixa potência incidente é devido ao estágio de amplificação mostrado na figura 1 que tem um ganho DC maior que zero. Mesmo que não tenha luz chegando ao fotodiodo, a tensão de saída é 3,68V. Por outro lado, para valores elevados de potência, o amplificador satura, pois sua tensão de saída não pode ser maior que a tensão de alimentação, 10V. Portanto, quanto maior a potência óptica de entrada, a resposta irá tender ao valor ideal de $10\text{V}/2,2\text{mA}$.

8.3 Aplicação em Sistemas de Comunicações Ópticas

Em sistemas de comunicações analógicas, o circuito eletrônico da Figura 8.1 é suficiente para usos em taxas menores que 1GHz. Nesse caso, as variações ópticas no intervalo de 0mW a 2,2mW são convertidas para uma variação de tensão no intervalo de 3,68V a 8,44V. Por outro lado, se o receptor é empregado em sistemas de comunicações digitais, é necessário o circuito adicional mostrado na Figura 8.9. Basicamente, a digitalização é realizada pelo flip-flop PECL ELT51. O uso de lógica PECL possibilita a utilização de uma fonte de tensão de 5V, em vez de uma simétrica (+5,-5V), tomando proveito da alta velocidade da família de lógica ECL. O circuito da Figura 8.9 pode detectar pulsos ópticos com larguras abaixo de 10ns.

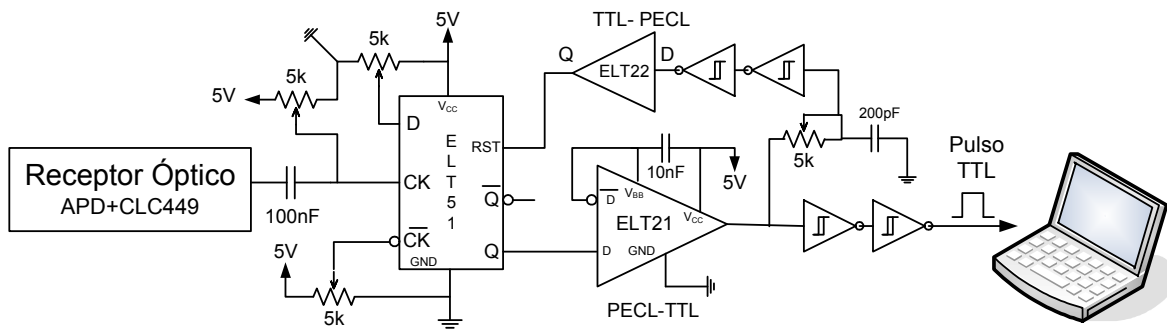


Figura 8.9: Circuito que fornece um pulso TTL de largura controlável na saída para cada avalanche.

Como exemplo, a Figura 8.10 mostra o pulso que modula o laser (1) e o pulso na entrada não inversora do amplificador operacional da Figura 8.1 (2). Já na Figura 8.11, o pulso TTL na saída do detector da Figura 8.9 (1) e o pulso amplificado na saída do amplificador (2). Sendo assim, como pode ser visto nas Figuras 8.10 e 8.11, o circuito eletrônico proposto trabalha como esperado e pode ser usado em sistemas de comunicações ópticas. Também pode ser observado que o pulso amplificado é mais largo que o pulso na entrada do amplificador. Isto ocorre porque quanto maior o ganho, mais estreita é a banda. No nosso caso, o ganho foi de 4,5 e, portanto, a largura foi mais estreita do que o valor de 1,2GHz quando o ganho é 2.

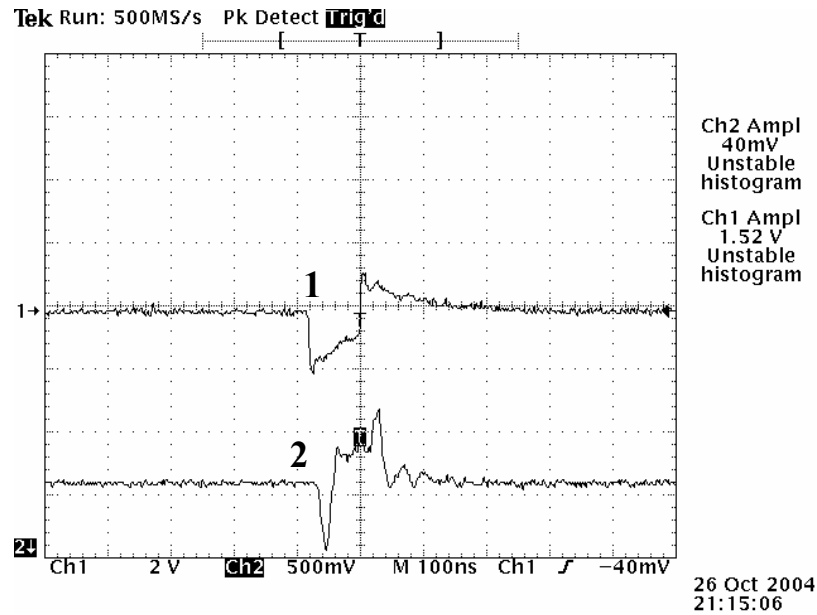


Figura 8.10: Pulso elétrico que modula o diodo laser (1) e sinal elétrico na entrada não-inversora amplificador operacional (2).

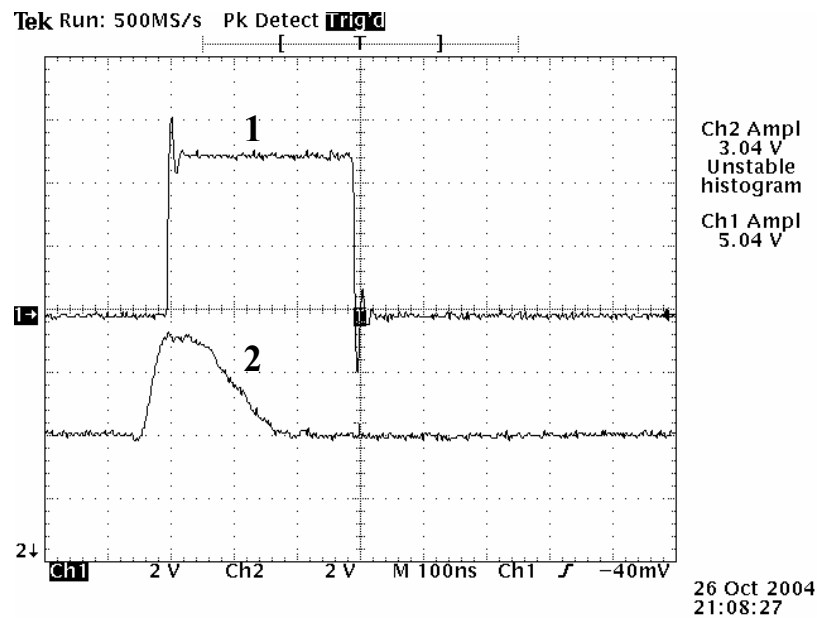


Figura 8.11: Pulso TTL na saída do detector (1) e o sinal amplificado na saída do amplificador operacional (2).

Capítulo 9

CONCLUSÕES E PERSPECTIVAS

Nos Capítulos 1 e 2 foram revisados conceitos de teoria da distribuição quântica de chaves e as suas principais implementações com estados coerentes fortemente atenuados. Dentre estes, destacam-se o plug&play com interferômetro de Mach-Zehnder pela estabilidade e facilidade de implementação, o sistema que utiliza codificação de fase entre bandas laterais de frequência, pois permite uma ampliação usando mais portadoras e o sistema polarimétrico de alta velocidade.

No Capítulo 3 é mostrada analiticamente a possibilidade da implementação paralela de dois protocolos BB84 com o sistema de modulação de fase relativa com duas portadoras de RF, um modulador de amplitude em Alice e um modulador de fase em Bob. Isso só é possível por que as interferências entre as bandas laterais são independentes para cada portadora.

No Capítulo 4, foi mostrada a implementação e os resultados experimentais de um sistema óptico executando o protocolo de DQC B92 polarimétrico. Os resultados das curvas de probabilidade de detecção dos detectores e de taxa de erro do sistema são bastante claros, mostrando que o sistema funciona como esperado, mesmo com estabilidade e desempenho baixos. A taxa de erro obtida, considerada alta em relação a outros sistemas já realizados, é decorrente das rotações de polarização não corrigidas causadas pelos dispositivos ópticos usados nos experimentos e do efeito da despolarização da luz durante propagação na fibra óptica.

No Capítulo 5 são introduzidos os conceitos de polarização quântica de estados coerentes essenciais para o entendimento do sistema de encriptação física de dados usando estados coerentes mesoscópicos. A segurança deste sistema é baseada no fato de que estados coerentes não são perfeitamente distinguíveis e na não comutabilidade dos parâmetros \hat{S}_1 , \hat{S}_2 e \hat{S}_3 de Stokes. Assim, usando prudentemente a combinação entre o número médio fótons por pulso e o número de bases usadas na modulação, a probabilidade

de erro para um espião que tente ler os bits encriptados tende a 50%. No entanto, o sistema não detecta a presença de intrusos.

No Capítulo 6 foi feita a análise da utilização de esquemas ativo e passivo de correção de erros no sistema de encriptação física com estados coerentes mesoscópicos. A análise mostrou que os sistemas de correção de erro são úteis e, no caso do passivo, pode ser facilmente empregado.

No Capítulo 7, combinando o protocolo de encriptação física com estados coerentes mesoscópicos e a DQC com estados coerentes fortemente atenuados, é possível a implementação de um sistema de DQC híbrido. No protocolo híbrido, como nenhum bit é perdido, uma vez que Alice e Bob escolhem a mesma base sempre, a taxa de transmissão de bits úteis dobra em relação ao BB84 original. Além disso, a utilização de memória quântica por parte de Eva num possível ataque será inútil, pois Alice e Bob não mais divulgarão as bases utilizadas. Por fim, é também mostrado que o sistema híbrido pode também ser diretamente utilizado na implementação de um protocolo de autenticação quântica de mensagens clássicas.

Por fim, no Capítulo 8 foi feita a análise teórica e experimental detector de pulsos ópticos para uso em comunicações ópticas e que servirá de instrumento para futuros experimentos no LATIQ/DETI da UFC. Além disso, com a determinação experimental da responsividade do fotodiodo PIN que é usado pelo receptor, foi possível estimar a energia do pulso óptico e, conseqüentemente, o número médio de fótons que é usado como parâmetro nos experimentos do Capítulo 4.

Como perspectivas de trabalhos futuros podem ser citadas: 1) Montar um sistema de DQC de melhor desempenho e que execute também o protocolo BB84, polarimétrico e interferométrico. 2) Fazer uma análise rigorosa da segurança dos diversos tipos de sistemas de DQC existentes contra ataques do tipo Trojan horse, separação de fótons com e sem maquina de clonagem, bem como propor sistemas de fácil implementação que sejam resistentes a estes tipos de ataques. 3) Fazer uma análise das dificuldades, vantagens e desvantagens da implementação de um sistema de DQC baseado na fase relativa de bandas laterais com duas portadoras de RF e moduladores de amplitude e fase. 4) Fazer uma análise das dificuldades, vantagens e desvantagens da implementação de um sistema de DQC híbrido.

REFERÊNCIAS

- [1] N. Gisin, G. Ribordy, W. Tittel e H. Zbinden, “Quantum Cryptography”, *Rev. of Modern Physics* 74, pp. 145-195, 2002.
- [2] S. Sing, “O livro dos códigos”, 2ª edição, Ed. Record, Rio de Janeiro, 2002.
- [3] H. Zbinden, H. Bechmann-Pasquinucci, N. Gisin e G. Ribordy, “Quantum Cryptography”, *Appl. Phys. B* 67, pp. 743-748, 1998.
- [4] D. Ljunngren, “Protocols in Quantum Cryptography Systems: Implementation of Software for Secret Key Extraction”, *Dissertação de Mestrado, Laboratory of Photonics and Microwave Engennering, Department of Electronics, Kungl Tekniska Hogskolan (KTH)*, 1999.
- [5] S. J. D. Phoenix, P. D. Townsend, “Quantum Cryptography: How to beat the code breakers using quantum mechanics”, *Cont. Phys.* 36 (3), pp. 163-195, 1995.
- [6] Ch. Marand, P. D. Townsend, “Quantum Key Distribution over Distances as 30 km”, *Opt. Lett.* 20 (16), pp. 1695-1697, 1995.
- [7] P. D. Townsend, “Quantum Cryptography on optical fiber networks”, *Opt. Fiber Technology*, 4, pp. 345-370, 1998.
- [8] A. Muller, T. Herzong, B. Huttner, W. Tittel, H. Zbinden e N. Gisin, “Plug and play systems for quantum cryptography”, *Appl. Phys. Lett.* 70(7), pp. 793-795, 1997.
- [9] H. Zbinden, J. D. Gautier, N. Gisin, B. Huttner, A. Muller e W. Tittel, “Interferometry with faraday mirrors for quantum cryptography”, *Electron. Lett.* 33 (7), pp. 586-588, 1997.
- [10] H. Zbinden, N. Gisin, B. Huttner, A. Muller e W. Tittel, “Practical aspects of quantum cryptographic key distribution”, *Journal of Cryptology* (2000), 13, pp. 207-220.
- [11] G. Ribordy, J. D. Gautner, N. Gisin, O. Guinnard e H. Zbinden, “Automated ‘Plug&Play’ quantum key distribution”, *Electron. Letters*, 34 (22), pp. 2116-2117, 1998.
- [12] D. Stucki, N. Gisin, O. Guinnard, G. Ribordy e H. Zbinden, “Quantum key distribution over 67 km with a plug&play system”, *New Journal of Physics*, 4, pp. 41.1-41.8, 2002.
- [13] J.-M. Mérola, Y. Mazurenko, J.-P. Goedgebuer, L. Duraffourg, H. Porte e W. T. Rhodes, “Quantum cryptography device using single-photon phase modulation”, *Physical Review A*, 60 (3), pp. 1899-1905, 1999.

- [14] J.-M. Mérolla, Y. Mazurenko, J.-P. Goedgebuer e W. T. Rhodes, “Single-photon interference in sidebands of phase-modulated light for quantum cryptography”, *Physical Review Letters*, 82 (8), pp. 1656-1659, 1999.
- [15] L. Duraffourg, J.-M. Mérolla, J.-P. Goedgebuer, Y. Mazurenko e W. T. Rhodes, “Compact transmission system using single sideband modulation of light for quantum cryptography”, *Opt. Letters*, 26 (18), pp. 1427-1429, 2001.
- [16] J.-M. Mérolla, L. Duraffourg, J.-P. Goedgebuer, A. Soujaeff, F. Patois e W. T. Rhodes, “Integrated quantum key distribution system using single sideband detection”, *Eur. Phys. J. D*, 18, pp. 141-146, 2002.
- [17] O. L. Guerreau, J.-M. Mérolla, A. Soujaeff, F. Patois, J.-P. Goedgebuer e F. J. Malassenet, “Long distance QKD transmission using single-sideband detection scheme with WDM synchronization”, *IEEE Journal of Selected Topics in Quantum Electronics*, 9 (6), pp. 1533-1540, 2003.
- [18] G. B. Xavier, “Esquemas de modulação para distribuição quântica de chaves com codificação de frequência”, *Dissertação de Mestrado*, Pontifícia Universidade Católica do Rio de Janeiro, 2005.
- [19] K. J. Gordon, V. Fernandez, G. S. Buller, I. Rech, S. D. Cova, e P. D. Townsend, “Quantum key distribution system clocked at 2GHz”, *Optics Express*, vol. 13, N° 8, 3015-3020, 2005.
- [20] K. J. Gordon, V. Fernandez, P. D. Townsend, e G. S. Buller, “A short wavelength gigahertz clocked fiber-optic quantum key distribution system”, *IEEE Journal of Quantum Electronics*, vol. 40, N° 7, 900-908, 2004.
- [21] J. C. Bienfang, A. J. Gross, A. Mink, B. J. Hershman, A. Nakassis, X. Tang, R. Lu, D. H. Su, C. W. Clark, C. J. Williams, E. W. Hagley e J. Wen, “Quantum key distribution with 1.25 Gbps clock synchronization”, *Optics Express*, vol. 12, N° 9, 2011-2016, 2004.
- [22] Tsuyoshi Nishioka, Hirokazu Ishizuka, Toshio Hasegawa, e Jun’ichi Abe, *Circular Type Quantum Key Distribution*, *IEEE Photonics Technology Letters*, vol. 14, no. 4, April, 2002.
- [23] Bing Qi, Lei-Lei Huang, Hoi-Kwong Lo, Li Qian, *Quantum key distribution based on a Sagnac loop interferometer and polarization-insensitive phase modulators*, xxx.lanl.gov/quant-ph/0604187, 2006.

- [24] H. K. Lo e H. F. Chau, *Science*, vol. 283, p. 2050, 1999.
- [25] P. W. Shor e J. Preskill, *Physical Review Letters*, vol. 85, p. 441, 2000.
- [26] K. Tamaki, M. Koashi, and N. Imoto, Unconditionally secure key distribution based on two non-orthogonal states, <http://xxx.lanl.gov> – quant-ph/0212162, 2003.
- [27] K. Tamaki e N. Lütkenhaus, Unconditional security of the Bennet 1992 protocol quantum key-distribution over lossy and noisy channel. <http://xxx.lanl.gov> – quant-ph/0308048, 2003.
- [28] D. F. Walls e G. J. Milburn, *Quantum Optics*, Springer-Verlag, 2^a Ed. 1995.
- [29] A. Acín, N. Gisin, e V. Scarani, Coherent pulse implementations of quantum cryptography protocols resistant to photon number splitting attacks, <http://xxx.lanl.gov> – quant-ph/0302037, 2003.
- [30] Y.-G. Tan e Q.-Y. Cai, Photon-number-solving decoy state quantum key distribution, <http://xxx.lanl.gov> – quant-ph/0508099, 2005.
- [31] C.-Z. Peng, J. Zhang, D. Yang, W.-Bo Gao, H.-X. Ma, H. Yin, H.-P. Zeng, T. Yang, X.-B. Wang, e J.-W. Pan, <http://xxx.lanl.gov> – quant-ph/0607129, 2006.
- [32] A. Ortigosa-Blanch e J. Capmany, “Subcarrier multiplexing optical quantum key distribution”, *Physical Review A*, vol. 73, p. 024305, 2006.
- [33] G. A. P. Thé, “Teoria e implementação de detectores de fótons isolados para comunicações quânticas em redes ópticas”, Dissertação de Mestrado, Universidade Federal do Ceará, 2006.
- [34] M. O. Scully, M. S. Zubairy, “*Quantum Optics*”, Cambridge University Press, 1997.
- [35] B. A. Robson, “*The theory of polarization phenomena*”, Clarendon Press, Oxford, 1974.
- [36] P. Usachev, J. Söderholm, G. Björk e A. Trifonov, “Experimental verifications of differences between classical and quantum polarization properties”, *Opt. Commun.*, 193, pp. 161-173, 2001.
- [37] G. S. Agarwal, J. Lehner e H. Paul, “Invariances for states of light and their quasi-distributions”, *Opt. Commun.*, 129, pp. 369-372, 1996.
- [38] H. Prakash e N. Chandra, “Density operator of unpolarized radiation”, *Phys. Rev. A*, 4, pp. 796-799, 1971.
- [39] J. Lehner, U. Leonhardt e H. Paul, “Unpolarized light: classical and quantum states”, *Phys. Rev. A*, 53, pp. 2727-2735, 1996.

- [40] G. A. Barbosa, E. Corndorf, P. Kumar e H. P. Yuen, “Secure communication using coherent states”, arXive e-print quant-ph/0210089 v2 (28 Jul 2003).
- [41] G. A. Barbosa, E. Corndorf, P. Kumar e H. P. Yuen, “Secure communication using mesoscopic coherent states”, *Phys. Rev. Letters*, 90, 227901, 2003.
- [42] G. A. Barbosa, “Fast and secure key distribution using mesoscopic coherent states of light”, *Phys. Rev. A*, 68, 052307, 2003.
- [43] G. A. Barbosa, “Information theory for key distribution systems secured by mesoscopic coherent states”, *Phys. Rev. A*, 71, 062333, 2005.
- [44] C. W. Helstrom, “Quantum detections and estimation theory”, Series: Mathematics in Science and Engineering, Academic Press, 1976.
- [45] D. Kalamidas, “Single-photon quantum error rejection and correction with linear optics”, *Phys. Lett. A* 343, p. 331-335, 2005.
- [46] Brito, D.B., Ramos, R.V., “Passive quantum error correction with linear optics”, *Physics Letters A*, 352, 3, 27, Pg 206-209, March 2006.
- [47] J. C. do Nascimento, “Correção de Erro em Sistemas de Comunicação Quântica Utilizando Polarização de Estados Coerentes e Fótons Isolados”, Dissertação de Mestrado apresentada no Departamento de Engenharia de Teleinformática, Universidade Federal do Ceará, 2006.
- [48] J. C. do Nascimento, F. A. Mendonça and R. V. Ramos, “Linear optical setups for active and passive quantum error correction in polarization encoded qubits”, Submetido a *Physics Letters A*, 2006.
- [49] H. P. Yuen, P. Kumar, E. Condorf, e R. Nair, “Security of Y-00 and similar quantum cryptographic protocols”, xxx.lanl.gov – quant-ph/0407067, 2004.
- [50] H. P. Yuen, “On the security of Y-00 under fast correlation and other attacks on the key”, xxx.lanl.gov – quant-ph/0608028, 2006.
- [51] T. Nishioka, T. Hasegawa, H. Ishizuka, K. Imafuku, e H. Imai, “How much security does Y-00 protocol provide us?”, *Physics Letters A*, vol. 327, p. 28-32, 2004.
- [52] H. P. Yuen, P. Kumar, E. Condorf, e R. Nair, Comment on: ‘How much security does Y-00 protocol provide us?’, *Physics Letters A*, vol. 346, p. 1-6, 2005.

- [53] T. Nishioka, T. Hasegawa, H. Ishizuka, K. Imafuku e H. Imai, Reply to: “Comment on: ‘How much security does Y-00 protocol provide us?’ ”, *Physics Letters A*, vol. 346, p. 7-16, 2005.
- [54] Z. L. Yuan e A. J. Shields, Comment on “Secure communication using mesoscopic coherent states”, *Physical Review Letters*, vol. 94, p. 048901, 2005.
- [55] H. P. Yuen, “Direct use of secret key in quantum cryptography”, xxx.lanl.gov – quant-ph/0603264, 2006.
- [56] H. P. Yuen, “KCQ: a new approach to quantum cryptography I. General principles and key generation”.
- [57] Rex Antônio da Costa Medeiros, “Protocolo para Autenticação Quântica de Mensagens Clássicas”, Dissertação de Mestrado, Departamento de Engenharia Elétrica, Universidade Federal de Campina Grande, 2004.
- [58] F. A. Mendonça, R. V. Ramos, “Optical receiver for instrumentation and communication”, *Microwave and Optical Technology Letters*, vol. 45, 5, pp. 415-419, 2005.