PONTIFÍCIA UNIVERSIDADE CATÓLICA DE CAMPINAS

CENTRO DE CIÊNCIAS EXATAS AMBIENTAIS E DE TECNOLOGIAS

RODRIGO FRANDSEN DA SILVA

ANÁLISE DE CRIPTOGRAFIA ÓPTICA REALIZADA MEDIANTE CONTROLE DA AMPLITUDE E DO ATRASO DE FATIAS ESPECTRAIS GERADAS COM PERFIL DE FILTROS ÓPTICOS COMERCIAIS

CAMPINAS

2012

RODRIGO FRANDSEN DA SILVA

ANÁLISE DE CRIPTOGRAFIA ÓPTICA REALIZADA MEDIANTE CONTROLE DA AMPLITUDE E DO ATRASO DE FATIAS ESPECTRAIS GERADAS COM PERFIL DE FILTROS ÓPTICOS COMERCIAIS

Dissertação apresentada ao Centro de Ciências Exatas, Ambientais e de Tecnologias - CEATEC, da Pontifícia Universidade Católica – PUC - Campinas, como requisito parcial à obtenção do título de Mestre em Gerência de Redes de Telecomunicações.

Orientador: Prof. Dr. Marcelo Luís Francisco Abbade

PUC-CAMPINAS

2012

RODRIGO FRANDSEN DA SILVA

ANÁLISE DE CRIPTOGRAFIA ÓPTICA REALIZADA MEDIANTE CONTROLE DE APLITUDE E DO ATRASO DE FATIAS ESPECTRAIS GERADAS COM PERFIL DE FILTROS ÓPTICOS COMERCIAIS

Dissertação apresentada ao Curso de Mestrado Profissional em Gestão de Redes de Telecomunicações do Centro de Ciências Exatas, Ambientais e de Tecnologias da Pontifícia Universidade Católica de Campinas como requisito parcial para obtenção do título de Mestre em Gestão de Redes de Telecomunicações.
Área de Concentração: Gestão de Redes e Serviços.
Orientador: Prof. Dr. Marcelo Luís Francisco Abbade.

Dissertação defendida e aprovada em 19 de dezembro de 2012 pela Comissão Examinadora constituída dos seguintes professores:

_____
Prof. Dr. Marcelo Luís Francisco Abbade
Orientador da Dissertação e Presidente da Comissão Examinadora
Pontifícia Universidade Católica de Campinas

_____
Prof. Dr. Alexandre de Assis Mota
Pontifícia Universidade Católica de Campinas

_____
Prof. Dr. Ben-Hur Viana Borges
Universidade de São Paulo - Escola de Engenharia de São Carlos.

AGRADECIMENTOS

Primeiramente aos meus pais, Benedito e Maria Helena, o meu mais profundo agradecimento por todo apoio dado durante toda a minha vida.

À minha esposa Juliana, por toda a compreensão e incentivo durante todo o período.

A todos meus professores que me ajudaram alcançar meus objetivos, em especial ao meu professor orientador, Marcelo Luís Francisco Abbade, pela oportunidade, pela orientação, pelo exemplo de profissionalismo.

Ao meu colega de estudos e amigo, Luiz Antonio Fossaluzza Junior, pelas valiosas contribuições para esta dissertação.

Aos funcionários da Pontifícia Universidade Católica de Campinas, em especial aos técnicos do laboratório Juliana e Eduardo, que me ajudaram criando condições para que eu desenvolvesse este trabalho.

À Pontifícia Universidade Católica de Campinas, por ter propiciado a infraestrutura necessária, ambiente, e pela bolsa de estudos para que eu pudesse desenvolver este trabalho.

À FAPESP e ao CNPq pelo financiamento parcial deste trabalho, no âmbito do programa Fotonicom dos Institutos Nacionais de Ciência e Tecnologia.

“Quando a dor de não estar vivendo
for maior que o medo da mudança, a
pessoa muda.”

(Freud)

RESUMO

DA SILVA, Rodrigo Frandsen (2012). Análise de criptografia óptica realizada mediante controle da amplitude e do atraso de fatias espectrais geradas com perfil de filtros ópticos comerciais. Dissertação (Mestrado) de Conclusão de Curso para o Mestrado em Gerência de Redes de Telecomunicações. Campinas, 2012.

Neste trabalho avaliamos uma técnica para realizar a criptografia totalmente óptica em redes ópticas transparentes. Dessa maneira, pretende-se impedir que um intruso consiga capturar e analisar o sinal óptico. A técnica consiste em dividir um sinal óptico em diversas fatias espectrais e aplicar diferentes atenuações e atrasos a cada uma delas. Após este processo o sinal é novamente multiplexado e transmitido por uma rede óptica transparente. Neste ponto o sinal está idealmente ininteligível para qualquer receptor que não conheça a chave criptográfica (conjunto de atenuações e atrasos) utilizada. Para avaliar a força da chave criptográfica, mede-se a taxa de erros de bit (Bit Error Rate, BER) do sinal codificado, BER_C. De forma geral, quanto maior BER_C, menor é a chance de o sinal ser decodificado por um receptor não autorizado. Na decodificação o sinal é novamente dividido em fatias espectrais, e para todas as fatias são aplicados valores distintos de atenuação e atraso de forma a reconstituir o sinal de entrada. Na saída do decodificador, avalia-se a BER do sinal decodificado BER_D, que deve ser suficientemente baixa para permitir a recepção do sinal transmitido pela TON. Simulações com o *software* VPITransmissionMaker, da empresa VPIPhotonics Inc, foram utilizadas para investigar o desempenho da técnica para diferentes ganhos e atrasos. Para a operação de fatiamento espectral, os perfis dos filtros usados foram ajustados para representar equipamentos de mercado. Resultados indicam que BER_C pode atingir valores de até 42% e 32% para sinais com modulação *non return to zero - on-off keying* (NRZ-OOK) e por deslocamento de fase diferencial em quadratura (*differential quadrature phase shift keying*, DQPSK), respectivamente. Em ambos os casos foi possível encontrar resultados de

BER_D inferiores a 10^{-12}, mediante ajuste adequado do espaçamento entre os filtros, mesmo após 400 km de propagação por enlaces de fibra padrão. No melhor de nosso conhecimento, esta é a primeira vez que tais análises são apresentadas.

Palavras-chave: Criptografia Óptica, Codificação Óptica, Redes Ópticas Transparentes, Fatiamento Espectral.

ABSTRACT

DA SILVA, Rodrigo Frandsen (2012). Analysis of optical encryption performed by controlling the amplitude and delay of slices generated with spectral profile commercial optical filters. Dissertation (Master) End of Course for the Masters in Telecommunications Network Management. Campinas, 2012.

In this dissertation we evaluate a new technique that performs optical encryption of signals travelling through transparent optical networks (TON). It is, thus, intended to prevent eavesdroppers to capture and retrieve optical signals. The technique consists in dividing an optical signal into several spectral slices and applying different attenuation and delays to each of them. After this process the signal is again multiplexed and transmitted through the considered TON. At this point the signal is ideally unintelligible to any receiver who does not know the encryption key, i.e. the set of utilized attenuations and delays. To evaluate the strength of such key, we measure the bit error rate (Bit Error Rate, BER) of the encoded signal, BER_C. Generally speaking, the higher BER_C, the lower is the chance of the encrypted signal being decoded by an eavesdropper. At the authorized receiver side, signal is again divided into spectral slices which are subjected to a set of attenuations and delays that are complementary to the ones utilized as the encryption key. All slices are again multiplexed and, as a result, at the output of the decoder the original encoder input signal is ideally reconstructed. The quality of the decoded signal is measured by evaluating the BER of the decoded signal, BER_D, which should be low enough to allow proper reception of the signal transmitted by the TON. Simulations with the software VPITransmissionMaker, VPIPhotonics Company Inc., were used to investigate the performance of the technique for different gains and delays. For the operation of spectral slicing, the profiles of the utilized filters were adjusted to represent the ones of state-of-the-art off-the-shelf equipment. Results indicate that BER_C may reach values of up to 42% and 32% for non-return to zero (NRZ) and differential quadrature phase shift keying (DQPSK) signals, respectively. In both of these cases it was possible to find results of BER_D lower than 10^{-12}, after

properly adjusting the spacing between the filters; this was observed even for propagation over amplified standard fiber links with lengths as long as 400 km. To the best of our knowledge, this is the first time that such analyses are presented.

***Keywords**: Optical Encryption, Encryption Optics, Physical Layer, Transparent Optical Networks, Spectral Slicing.*

SUMÁRIO

LISTA DE FIGURAS

LISTA DE ACRÔNIMOS

ACRÔNIMO	TERMO	TERMO EM PORTUGUêS
BER	*Bit Error Rate*	Taxa de Erro de Bit
DCF	*Dispersion Compensation Fiber*	Fibra Compensadora de Dispersão
DP-DQPSK	*Dual-Polarization Differential Quadrature Phase Shift Keying*	Chaveamento por Desvio Diferencial de Quadratura de Fase em Polarização Dupla
DQPSK	*Differential Quadrature Phase Shift Keying*	Chaveamento por Desvio Diferencial de Quadratura de Fase
DSP	*Digital Signal Processing*	Processamento Digital de Sinais
EDFA	*Erbium Doped Fiber Amplifier*	Amplificador à Fibra dopada com Érbio
HTTPS	*Hypertext Transfer Protocol Secure*	
IPSec	*Internet Protocol Security*	Protocolos de Segurança da Internet
MAI	*Multiple-access Interference*	Interferência de Acesso Múltiplos
NRZ	*Non-return-to-zero*	
OCDMA	*Optical Code Division Multiple Access*	Acesso Múltiplo por Divisão de Código Óptico
ODL	*Optical Delay Line*	Linha de Atraso Óptico
OOK	*On-off keying*	
OSI	*Open System Interconnection*	Interconexão de Sistemas Abertos
PMD	*Polarization Mode Dispersion*	Dispersão dos Modos de Polarização
PRBS	*Pseudo-random Bit Sequence*	Sequência Pseudo-aleatória de Bit
SLM	*Spatial Light Modulator*	Modulador Espacial de Luz
TON	*Transparent Optical Networks*	Redes Ópticas Transparentes
VPN	*Virtual Private Network*	Redes Virtuais Privadas
WDM	*Wavelenght Division Multiplexing*	Multiplexação por Divisão de Comprimento de Onda

1 INTRODUÇÃO

O sigilo da informação tem se tornado um dos principais pontos de preocupação em todas as corporações. Visando manter as informações transmitidas confidenciais e não disponíveis para outros receptores indesejados a técnica de criptografar a mensagem tem se tornado cada vez mais utilizada. Grandes corporações já contam com sistemas de segurança da informação para trafegar suas informações pelas suas diversas filiais, possibilitando assim trocar dados sobre novos produtos, sem que concorrentes tenham acesso aos mesmos. Este fato está se tornando uma exigência no mercado devido ao grande volume de investimento exigido hoje para lançar um novo produto.

Este tema se torna mais importante com estudos (Em: <http://www.symantec.com/content/en/us/about/media/pdfs/b-ponemon-2011-cost-of-data-breach-global.en-us.pdf>. Acesso em: 1 dezembro 2012.) que demostram as sérias consequências financeiras a organizações que não mantêm seus dados protegidos e seus sistemas de comunicação seguros contra acesso de terceiros não autorizados. De fato, estes demonstram que o custo médio das falhas com segurança em 2011 foi de US$ 194,00 por consumidor. A mesma pesquisa indica que o custo médio organizacional com falhas de segurança em 2011 foi de 5,5 milhões de dólares por incidente. Este estudo ainda demonstra que dentre as empresas pesquisadas em 2011, a principal ação de mitigação após a ocorrência de uma brecha de segurança é investir em treinamento e sensibilizar os funcionários. A seguir, investe-se no uso da criptografia. A gravidade da situação pode ser notada pelo fato que uma única empresa teve gastos de 31 milhões de dólares para sanar uma única falha de segurança (Em: <http://www.ciena.com/connect/blog/Enterprises-face-huge-costs-with-threat-of-data-theft.html>. Acesso em: 1 dezembro 2012.). Os dados de 2012 ainda não estão consolidados, porém, o centro americano de identificação de roubo de recursos já registra para o ano de 2012 mais de 10

milhões de registros expostos por mais de 300 brechas de segurança (Em: <http://www.idtheftcenter.org/ITRC%20Breach%20Stats%20Report%202012.pdf>. Acesso em: 1 dezemro 2012.). Estes dados revelam a importância do tema e dos problemas que podem ser gerados pela falta de segurança da informação trafegada.

Devido à expansão na utilização de redes de comunicação, órgãos reguladores e governos estão (Em: <http://www.fas.org/sgp/crs/misc/R42338.pdf>. Acesso em: 1 dezembro 2012.) (Em: <http://www.aneel.gov.br/cedoc/ren2012502.pdf>. Acesso em: 1 dezembro 2012.) cada vez mais se preocupando com o assunto de segurança e privacidade da informação. De fato, mesmo setores que não estão diretamente ligados às telecomunicações, como as concessionárias de água e energia começaram a adotar redes de comunicação (Em: <http://www.cpfl.com.br/SaladeImprensa/Releases/tabid/154/EntryId/415/CPFL-anuncia-projetos-para-tornar-sua-rede-mais-eficiente-com-a-IBM-Brasil.aspx>. Acesso em: 1 dezembro 2012.) para automatizar serviços, como leitura de medidores. Estas redes de comunicação em geral são uma extensão da rede corporativa, às quais estão conectados computadores localizados em subestações e usinas. Esses computadores podem por ventura gerar comandos a equipamentos seccionadores que são importantes para todo sistema de distribuição. Por esta razão, a leitura não autorizada destes comandos pode permitir que intrusos causem danos a essas redes. Além disso, essas redes também podem trafegar dados relativos à cobrança e a fatura das empresas atendidas pela rede.

Diante destas preocupações, fica claro que empresas de todos os segmentos enxergam a necessidade de investimento em segurança da infraestrutura de rede (lógica e física). Uma peça importante dos sistemas de informação é a infraestrutura de comunicação, onde todos os dados são trafegados. Apesar dos dados serem altamente protegidos em grandes

infraestruturas de *datacenters*, é essencial que os mesmos sejam trafegados por um canal seguro. É sabido que hoje grande parte da infraestrutura de redes de comunicação usadas pelas corporações é de uso público e por isso está fora do domínio da empresa.

A base da infraestrutura das redes de longo alcance é formada por redes ópticas, e dentre as tecnologias ópticas existentes se destaca as redes com multiplexação por divisão comprimento de onda (*Wavelenght Division Multiplexing*, WDM). De fato, a tecnologia WDM permite o uso de altas taxas de transmissão, em diferentes comprimentos de onda. Por exemplo, resultados atuais sugerem a viabilidade da transmissão de 80 canais de 100 Gbps em distâncias de até 1800 km (BIRK, 2011).

Em um cenário muito utilizado das redes ópticas, nonúcleo das redes de telecomunicações, as fibras ópticas são utilizadas para conectar equipamentos eletrônicos chamados de roteadores. Ao receber um dado sinal por uma fibra, estes roteadores convertem o sinal para o domínio elétrico, processam a informação (por exemplo, determinando uma rota de destino) e, após converter este sinal novamente para o domínio óptico, o envia por uma nova fibra. Durante o processamento, esses roteadores podem armazenar os dados e enviá-los para uma rota indevida. Isso claramente constitui uma brecha de segurança que não pode, em princípio, ser averiguada pelos clientes da rede.

Outro tipo de rede *core* que vem sendo adotada pelo mercado são as redes ópticas transparentes (*Transparent Optical Networks*, TONs). Nas TONs os dados são trafegados sem que haja a necessidade de conversão óptica – elétrica – óptica, diminuindo, assim, o uso de elementos eletrônicos, e por consequência a quantidade de elementos com inteligência embarcada. Assim, com a diminuição do uso de elementos eletrônicos, o roubo de informação se torna ainda mais difícil.

Porém, mesmo com a utilização de TONs é possível que sinais sejam indevidamente desviados. Isto pode ser feito por meio de métodos intrusivos ou não-intrusivos. No primeiro destes métodos, o sinal pode ser desviado por meio de divisores ópticos (*splitters*) para uma rota vizinha. Este tipo de técnica gera uma diminuição da potência do sinal recebido; porém, muitas vezes estas perdas de potência podem não ser percebidas pela operadora da rede. Em uma abordagem não-intrusiva pode-se utilizar equipamentos de mercado que empregam uma curvatura do cordão óptico, permitindo assim que o sinal óptico seja refratado para fora da fibra e detectado por algum equipamento não autorizado (SHANEMAN, 2004). De fato, estes equipamentos são facilmente encontrados, por um preço relativamente baixo (Em: <http://www.go4fiber.com/spec/PFC%201000.pdf>. Acesso em: 1 dezembro 2012).

Exemplos como os anteriores reforçam a importância de criptografar a informação e/ou os sinais que a representa. Comumente nos sistemas de tecnologia da informação, os canais de dados são criptografados na camada de apresentação do modelo de referência para interconexão de sistemas abertos (*Open System Interconnection*, OSI). Porém, quanto maior o número de camadas que contenham a criptografia, maior é o grau de segurança inferido no canal de comunicação (KITAYAMA, 2011; TANENBAUM, 2003; HARASAWA, 2011; CORNEJO, 2007). Em sistemas existentes já é possível combinar diversos tipos de criptografia aplicadas a diversas camadas, como com o uso de redes privadas virtuais (*Virtual Private Network*, VPN), que combinam os protocolos de segurança da internet (*Internet Protocol Security* - IPSec) com protocolos de aplicação seguros como HTTPS (*Hypertext Transfer Protocol Secure*).

Uma outra abordagem, além das mencionadas no parágrafo anterior, é realizar a criptografia (ou codificação) na camada física. Nesta linha, temos o exemplo da criptografia quântica. Esta técnica permite que ambos os lados da rede negociem a chave criptográfica no mesmo canal de comunicação, sem permitir que mesmo havendo um espião no canal, o mesmo possa descobrir a chave de comunicação. Esta técnica está em desenvolvimento e ainda está restrita a enlaces de aproximadamente 200 km (HARASAWA, 2011).

Outro exemplo de codificação na camada física é a utilização da tecnologia de acesso múltiplo por divisão de código óptico (*Optical Code Division Multiple Access* – OCDMA). O objetivo desta tecnologia é permitir que os dados de múltiplos usuários possam ser trafegados simultaneamente pelo mesmo canal óptico. Com esta técnica, o sinal de cada usuário do sistema de comunicação recebe um código, utilizado para distingui-lo dos sinais dos demais usuários. Apesar de eficiente no ponto de vista do compartilhamento de sinais, algumas das implementações desta técnica podem causar um espalhamento espectral do sinal óptico (SANTOS FILHO, 2006). Para redes WDM, o efeito do espalhamento espectral do sinal não é desejado causando incompatibilidades com as normas estabelecidas pelo ITU-T (ITU-T G.692) e, por conseqüência, com os equipamentos (multiplexadores e demultiplexadores) existentes no mercado para este tipo de rede.

Uma nova forma de criptografia na camada física voltada para redes WDM foi apresentada em (CORNEJO, 2007), utilizando uma técnica OCDMA voltada para um único usuário. Nesta técnica, sinais WDM são divididos em determinados intervalos de frequência (fatias espectrais) aos quais são aplicados diferentes deslocamentos de fase. O desempenho desta técnica foi analisado em termos da penalidade de olho experimentada por sinais *Non Return to Zero* (NRZ) de 10 Gbps após a decodificação.

Esta dissertação segue a técnica proposta em (ABBADE, 2012) na qual se realiza a codificação de sinais ópticos transportados em TONs. Nesta abordagem, divide-se o sinal em várias fatias espectrais, às quais são atribuídas analogicamente uma atenuação e um atraso. Após essa operação, as fatias espectrais são multiplexadas e passam a constituir uma versão distorcida do sinal original que pode, então, ser transmitido pela TON. Ao chegar ao seu destino, onde a chave é conhecida, o sinal pode ser novamente recomposto.

A técnica avaliada neste trabalho não causa espalhamento espectral do sinal, o que a torna compatível com canais WDM operando na grade do ITU-T . A referida técnica também é transparente para o tipo de modulação empregada no canal de comunicação.

A análise realizada neste trabalho compreendeu simulações para avaliar o desempenho da técnica considerada. Esta investigação possui vários elementos distintos de outros trabalhos da literatura (CORNEJO, 2007; LUIZ, 2012; ABBADE, 2012). Por exemplo, ao contrário do que ocorre em (CORNEJO, 2007), avalia-se também o desempenho do sinal codificado. Além disso, verifica-se a aplicabilidade da técnica proposta em sinais NRZ-OOK e DQPSK (Differential Quadrature Phase Shift Keying) com diferentes taxas de transmissão (20 e 40 Gbps). Diferente destes outros trabalhos, também considera-se que os filtros utilizados para o fatiamento espectral têm perfil correspondente ao de filtros reais encontrados no mercado.

Apesar de não terem sido realizados experimentos, as simulações devem oferecer resultados muito próximos aos reais, pois a técnica considerada é estritamente baseada em efeitos lineares. De fato, espera-se que trabalhos futuros possam analisar o desempenho experimental da técnica.

Esta dissertação está organizada da seguinte forma. No Capítulo 2 apresentam-se algumas características da aplicação de criptografia na camada física das redes de comunicação. No Capítulo 3 descreve-se a técnica criptográfica proposta. No Capítulo 4, o arranjo das simulações usadas para avaliar a técnica considerada é abordado. No Capítulo 5 apresentam-se os resultados obtidos utilizando a técnica proposta tanto em sistemas *back-to-back*, quanto em sistemas de transmissão óptica utilizando as modulações NRZ-OOK e DQPSK. No Capítulo 6 apresenta-se a conclusão do trabalho.

2 CODIFICAÇÃO NA CAMADA FÍSICA

Neste capítulo apresentam-se uma breve descrição de alguns métodos existentes de criptografia na camada física, mais especificamente em transmissões ópticas. A Seção 2.1 aborda uma técnica de criptografia quântica, considerada uma técnica de criptografia de chave única. A Seção 2.2 apresenta os princípios da tecnologia OCDMA. Na Seção 2.3, uma nova técnica de OCDMA que utiliza codificação por mudança de fase em diferentes fatias espectrais é discutida.

2.1 CRIPTOGRAFIA QUÂNTICA

Uma das formas conhecidas na literatura para realizar a codificação na camada física é a criptografia quântica. Uma importante característica desta técnica é que dois usuários de uma rede podem estabelecer uma comunicação sem ao menos terem qualquer contato prévio. Nesta seção aborda-se uma das formas de criptografia quântica, chamada de BB84 para indicar seus autores e o ano de publicação da proposta (BENNET E BRASSARD, 1984).

Esta técnica baseia-se no fato que a luz é transmitida por fótons que podem ser polarizados por um conjunto de filtros de polarização. Neste sentido, o transmissor do canal escolhe dois conjuntos de filtros de polarização. O primeiro conjunto consiste de dois filtros, um de polarização horizontal e outro de polarização vertical. Esta escolha é chamada de base retilínea. O segundo conjunto de filtros está deslocado 45º em relação ao primeiro e constitui a chamada base diagonal (TANENBAUM, 2003).

A seguir, o transmissor convenciona qual polarização representará os bits 0 e 1 em cada uma das bases. Por exemplo, na base retilínea o bit 0 é representado por um fóton com polarização vertical e o bit 1 é representado por um fóton com polarização horizontal. Na base diagonal o bit 0 é representado pelo fóton que emerge pelo filtro cuja polarização está estendida pelos quadrantes ímpares, ao passo que o bit 1 está representado pelo fóton que passa pelo filtro ortogonal a este. Após definir essas convenções, o transmissor as informa em texto simples para o receptor do canal.

Então, o transmissor escolhe uma sequência de bits aleatórios, e para cada bit desta sequência é selecionado aleatoriamente uma de suas bases. A Figura 1 apresenta um exemplo com 16 bits. Para transmitir cada bit o transmissor emite um fóton polarizado de acordo com a base convencionada (a). O receptor, com as mesmas configurações de bases de filtros escolherá ao acaso quais bases utilizar na recepção (b). Se escolher a base correta, receberá o bit correto, caso contrário ele receberá um bit aleatório. É importante notar que se o fóton passar por um filtro rotacionado a 45º da sua própria polarização seu estado se manterá ou será rotacionado em 90º com a mesma probabilidade. Neste estágio o receptor não sabe quais bits estão corretos e quais bits estão incorretos (c).

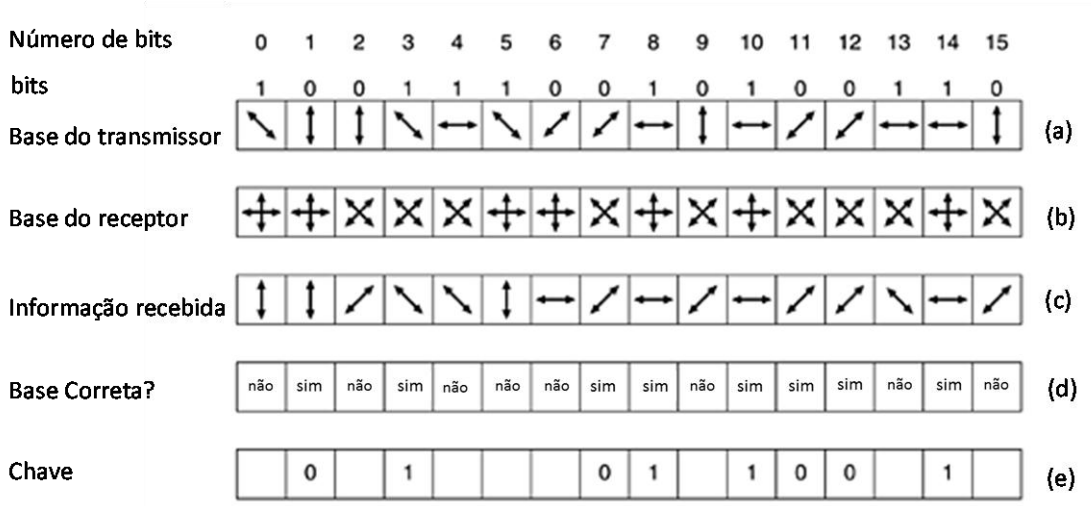

Figura 1 – Modelo de transmissão quântica.

No próximo passo o receptor então informa ao transmissor em texto simples, isto é, sem criptografia, quais bases foram utilizadas. O transmissor, sabendo quais as bases foram utilizadas para cada um dos bits, informa ao receptor em texto simples quais as bases estão corretas (d). Após o receptor receber essa informação, a chave criptográfica (e) única é definida a partir dos bits que foram identificados corretamente.

Nota-se que, mesmo se um intruso puder captar as mensagens enviadas nos dois sentidos (transmissor-receptor e receptor-transmissor), ele não poderá identificar com exatidão qual chave foi determinada. De fato, pode-se mostrar que, na média, este intruso acertará apenas metade dos bits desta chave. Além disso, a utilização de técnicas como a "amplificação de privacidade" (YUEN, 2006) pode reduzir ainda mais o número de bits da chave conhecidos pelo intruso.

Considerada uma maneira eficiente de criptografia na camada física, a criptografia quântica ainda está em fase de pesquisa. Com custos de implementação muito elevados e com restrições de propagação em enlaces ópticos (HARASAWA, 2011; TANAKA,2008; LADD, 2010), esta técnica ainda não pode ser considerada uma opção viável para transmissões ópticas comerciais.

A literatura apresenta outras técnicas de criptografia quântica, porém uma explicação mais aprofundada das mesmas está fora do objetivo deste trabalho.

2.2 ACESSO MÚLTIPLO POR DIVISÃO DE CÓDIGO ÓPTICO (OCDMA)

Ainda no estágio de pesquisa, o OCDMA pode prover uma forma conveniente de prover acesso a múltiplos usuários por meio de um mesmo

canal óptico (MUKHERJEE, 2006; ABDALLAH, 2011; HUISZOON, 2007). Nas redes OCDMA o sinal de vários usuários é codificado com códigos ortogonais na mesma banda. Nesta técnica o sinal só é recuperado se o receptor souber qual a chave foi usada para codificação do sinal.

Uma visão geral da topologia de uma rede OCDMA é mostrada no diagrama de blocos da Figura 2. Nesta rede cada usuário gera uma sequência de dadosque serão codificados por meio de uma palavra-chava. Após a codificação esses sinais são acoplados a sinais codificados de outros usuários e transmitidos por uma rede. Do outro lado somente o receptor que conhece a palavra-chave utilizada na codificação poderá recuperar o sinal adequadamente.

Essa tecnologia apresenta duas características importantes. A primeira é a ortogonalidade, que determinará o grau de diferenciação entre os códigos utilizados. A segunda é a cardinalidade, que corresponde ao número de códigos utilizados. Em principio, os códigos devem ter uma grande cardinalidade e uma boa autocorrelação (correlação com o próprio código) e boa correlação cruzada com os códigos de outros usuários, a fim de extrair o máximo em ortogonalidade.

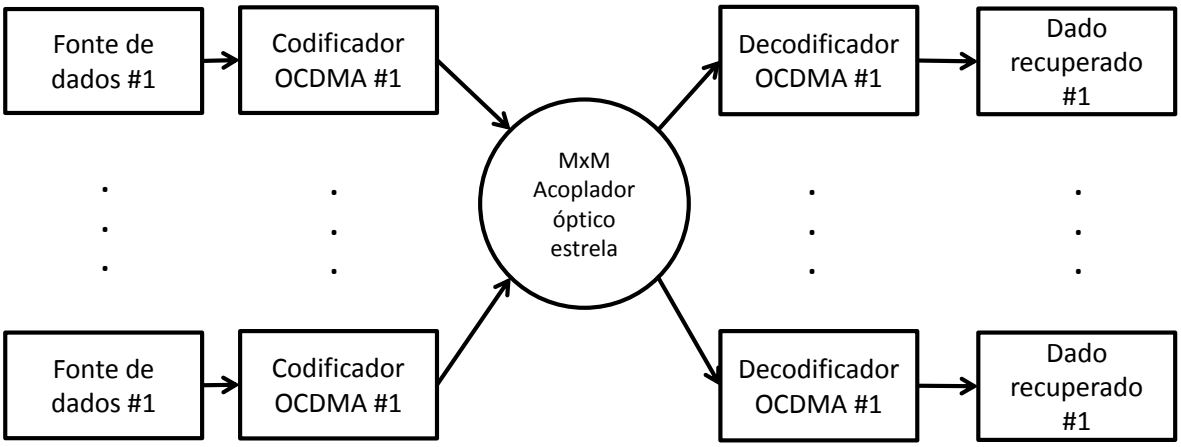

Figura 2 - Diagrama de blocos de um sistema OCDMA.

A literatura apresenta várias técnicas para implementar a codificação em redes OCDMA (YIN, 2007). Nesta seção, abordaremos apenas a codificação 1D incoerente em sinais *on-off keying* (OOK). Codificações 2D, coerentes e com outras variações estão além do escopo de nosso trabalho, mas podem ser encontradas em (YIN, 2007).

m uma rede OCDMA utilizando OOK cada bit 1 transmitido pelo usuário é codificado utilizando a palavra código assinalada a ele. Nesta abordagem, o bit 0 é enviado sem nenhum tipo de codificação. Na Figura 3 apresentamos um esquema deste tipo de codificação no domínio do tempo. Em uma transmissão, cada bit é transmitido por um período T_b (a). Em uma rede OCDMA, o período do bit T_b é subdividido em N intervalos T_c (b), denominados *chips* (REIS JR., 2009). A palavra código de cada usuário é determinada pela quantidade de chips iluminados w como também pela sequência dos mesmos no período do bit. A Figura 3 ilustra os sinais de 3 usuários (a), (b) e (c), cada qual com sua palavra código e compartilhando o mesmo meio de transmissão.

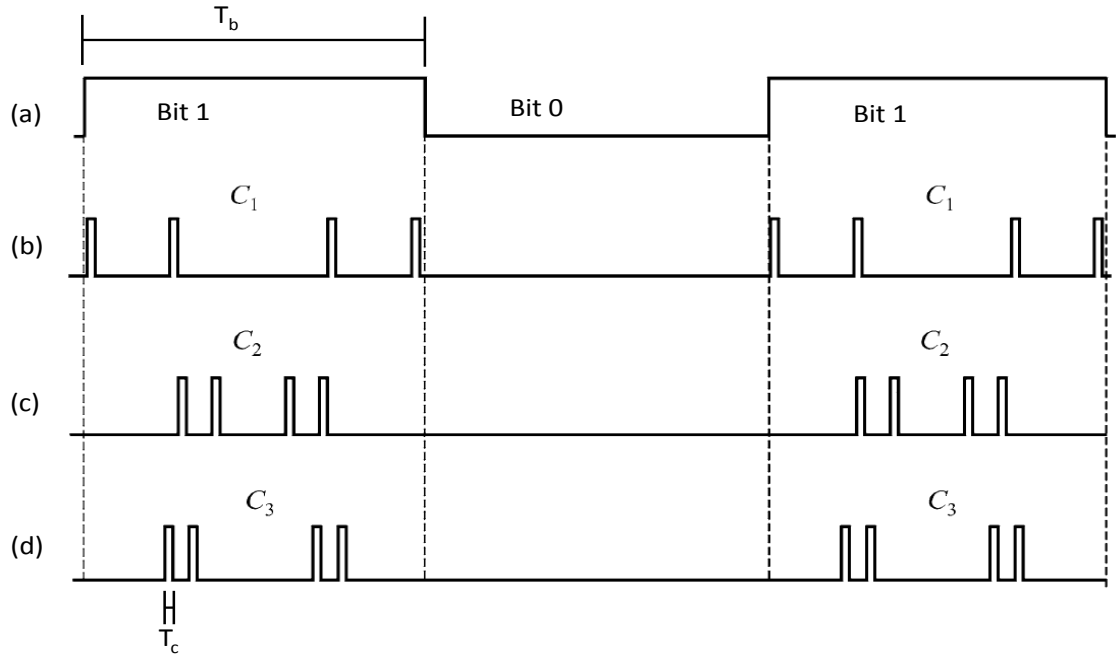

Figura 3 – Formas de onda codificadas pelas palavras código b, c e d.

Na Figura 4 exibe um diagrama esquemático de um codificador (a) e um decodificador (b) OCDMA. O codificador (a) consiste de um *splitter* óptico, de linhas ópticas de atraso (*optical delay lines*, ODL) e de um acoplador óptico. Um sinal de entrada correspondente a um único bit é divido em *N* partes, sendo que cada uma delas é submetida a seu próprio atraso $\tau = kT_c$, com $0 \leq k \leq N$. A seguir, estas partes são multiplexadas para constituir o sinal codificado. Por sua vez, este sinal pode ser transmitido pelo canal óptico, juntamente com o sinal codificado de outros usuários (KOSTINSKI, 2008; WANG, 2007; PRUCNAL, 2009; ETEMAD, 2007; YIN, 2007; CONCOTTI, 2008; WU, 2006; LOPES, 2005).

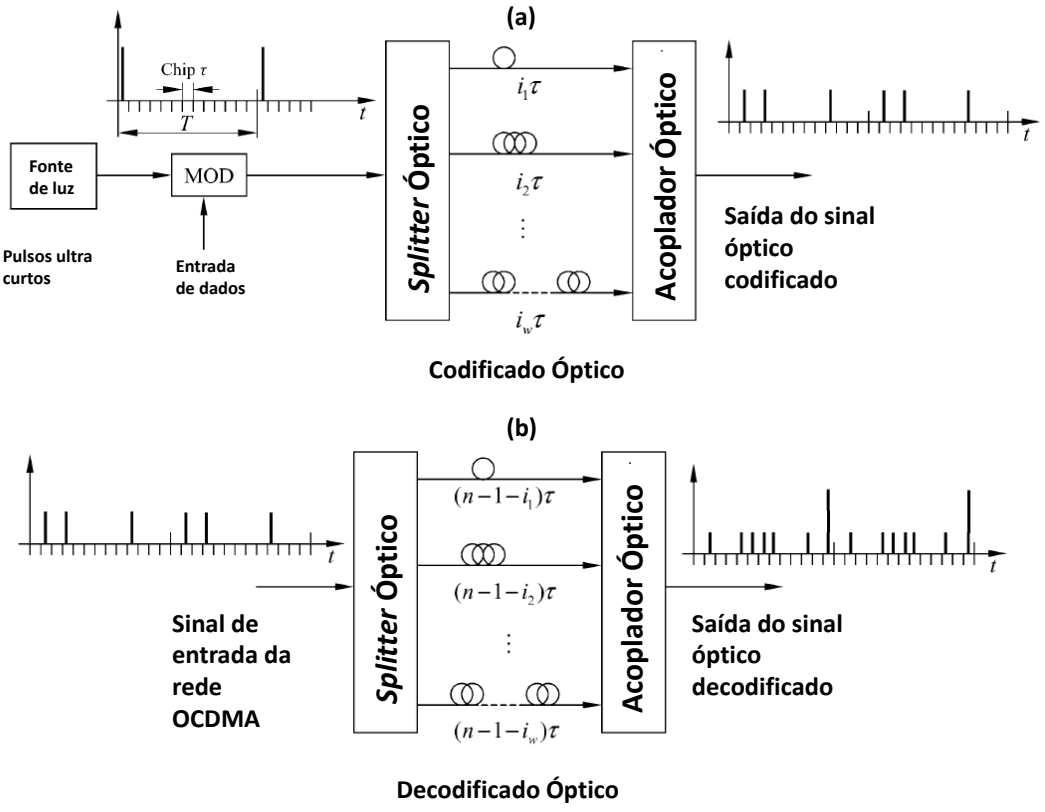

Figura 4 – Diagrama esquemático do codificador e decodificador OCDMA. Chips iluminados *w.* Numero de subintervalos *N.* Atraso τ.

Na recepção do sinal os usuários de cada destino conhecem o código implantado pelo transmissor correspondente. Assim, utilizando um dispositivo similar ao codificador (Figura 4 (b)), mas com linhas que oferecem um atraso de (N- 1- k) T_c, o sinal pode ser devidamente decodificado. Nota-se que o desempenho desta codificação pode ser afetado pela interferência de múltiplo acesso (*multiple-access interference*, MAI). Uma discussão aprofundada destes assunto está além do escopo deste trabalho e pode ser encontrada em (SANTOS FILHO, 2006; REIS JR., 2009; SALEHI, 1989).

Como $T_c < T_b$ a técnica provoca um espalhamento do sinal no domínio da frequência. Embora isso seja aceitável do ponto de vista de redes de acesso, nas quais as exigências sobre a eficiência espectral não são tão grandes, este tipo de alargamento não é admissível em redes *core* nas quais o uso de multiplexadores e demultiplexadores restringe a banda do sinal, tipicamente, a 50 GHz (ITU-T G.692).

2.3 CODIFICAÇÃO OCDMA POR DIFERENCIAÇÃO DE FASE

Uma nova proposta de codificação OCDMA, voltada para criptografia de sinais em redes WDM foi apresentada em (CORNEJO, 2007). Nesta técnica, conforme ilustrado na Figura 5, o sinal incide sobre uma grade de difração altamente dispersiva G1 que provoca uma dispersão do espectro do sinal de entrada (CORNEJO, 2007). O sinal refletido é então transmitido por uma lente convergente e, a seguir, é submetido a uma máscara de difração dispersiva de Bragg M, responsável por filtrar as componentes (pixel) do sinal. As fases de cada componente são alteradas pela aplicação de tensão a cada pixel. Após isso, o sinal é novamente transmitido por outra lente convergente, até a grade de difração G2. Após esse processo o sinal é então codificado e transmitido por uma fibra óptica. Nesta técnica, o sinal só é decodificado se o receptor conhecer

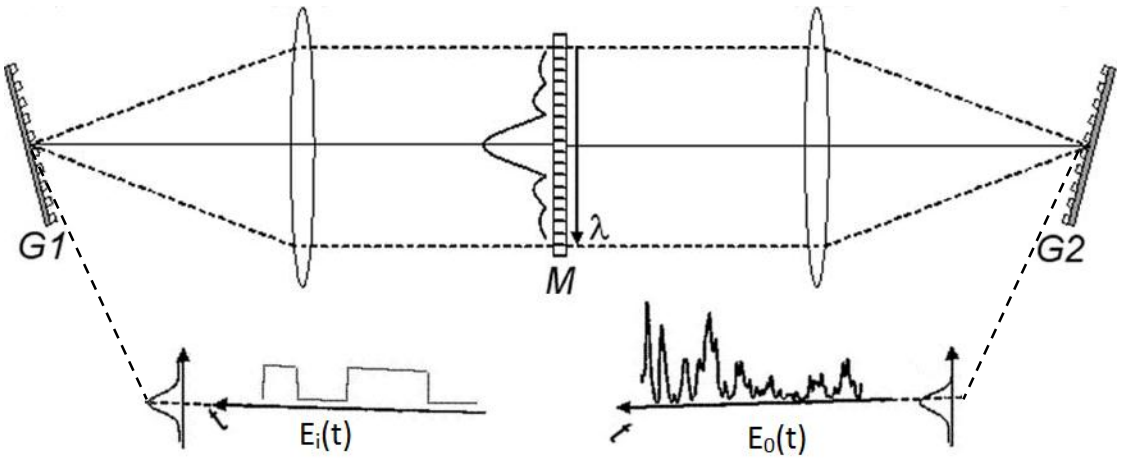

Figura 5 – Codificação por diferenciação de fase.

a quantidade e o tamanho de cada pixel, como também a tensão aplicada a ele, para que assim possa decodificar o sinal.

Apesar de esta técnica apresentar uma forma de codificar sinais WDM na camada física sem causar alargamento espectral, os autores se restringiram em analisá-la para sinais NRZ com taxa de transmissão de 10 Gbps, submetidos a filtros ideais e não consideraram o desempenho do sinal criptografado. Observa-se que as redes WDM atuais utilizam largamente sinais DQPSK. Além disso, a utilização de filtros reais pode afetar drasticamente o desempenho dos sinais codificados e decodificados. Como será mostrado nos capítulos a seguir, esta dissertação apresentará estas análises para a técnica proposta em (ABBADE, 2012).

3 MÉTODO CRIPTOGRÁFICO PROPOSTO

Neste capítulo apresenta-se uma descrição do método criptográfico considerado neste trabalho. Na Seção 3.1 descrevem-se os processos de codificação e decodificação. Na Seção 3.2 discutem-se algumas formas de prover o sincronismo entre o decodificador e o codificador.

3.1 DESCRIÇÃO DA TÉCNICA PROPOSTA

O sistema criptográfico proposto está ilustrado pelo diagrama de blocos da Figura 6. O sinal é dividido em *n* fatias espectrais, por meio de demultiplexador óptico ou por meio de um *splitter* óptico combinado com um conjunto de filtros ópticos passa-faixa. Cada fatia espectral é então atenuada por um fator α_i em dB e atrasado por um fator τ_i (*i*= 1, 2, ..., *n*). As fatias espectrais podem possuir diferentes larguras de banda, que devem ser dimensionadas para a aplicação da técnica e posterior detecção. Os valores máximos de atenuação e de atraso usados em cada chave criptográfica são chamados de α_{max} e τ_{max}, respectivamente.

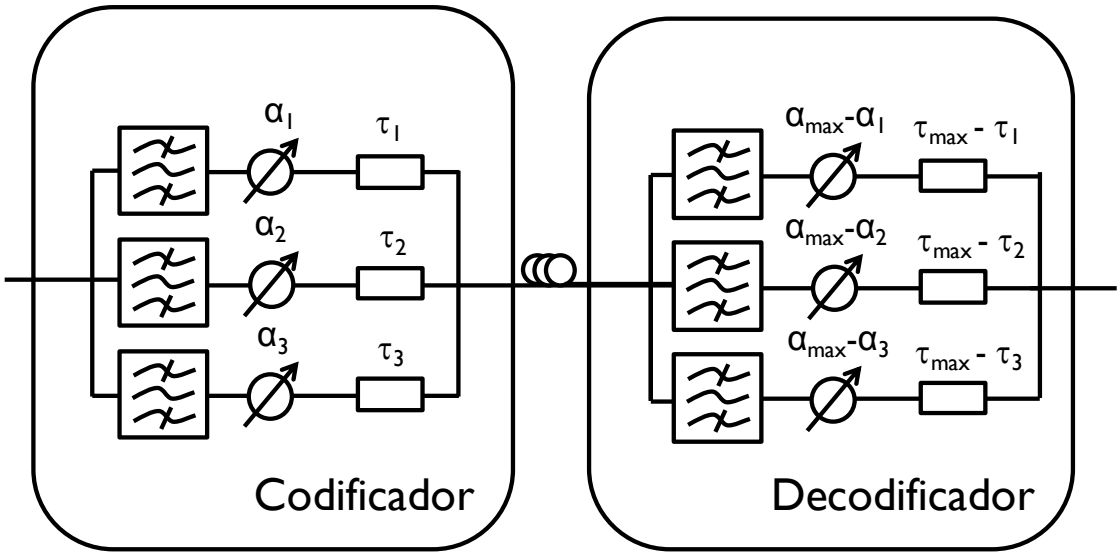

Figura 6 – Diagrama de blocos do sistema criptográfico proposto.

Após a aplicação da atenuação e do atraso, as fatias são novamente unidas por meio de um multiplexador óptico ou por meio de um acoplador óptico, opcionalmente, combinado com um conjunto de filtros ópticos (não ilustrados na Figura). O sinal codificado é então transmitido pela TON até o receptor. Para estabelecer se o sinal está adequadamente codificado é usada a medição da taxa de erro de bit (*bit error rate* – BER) do sinal codificado, BER_C. É importante destacar que para transmissão em um canal binário, a BER máxima é de 50 %. Nota-se que se um sinal tiver uma BER de 99 %, um inversor pode ser utilizado para transformar esta BER em 1%.

Na Figura 7, ilustra-se o efeito da técnica no espectro óptico, tanto no tempo quanto na amplitude. Os componentes da chave criptográficas da técnica variam de acordo com a complexidade desejada para o canal de comunicação. Em princípio, quanto maior o número de fatias espectrais e quanto mais distintas as atenuações e atrasos aplicados às fatias espectrais, mais difícil será para um intruso descobrir a chave criptográfica. Sabe-se hoje que existem filtros comerciais com largura de banda de 4 GHz (Em: <http://yenista.com/IMG/pdf/XTA-50_DS_201210.pdf>. Acesso em: 1 de Janeiro de 2013.), o que possibilitaria em principio a criação de 12 fatias espectrais em canais de 50 GHz.

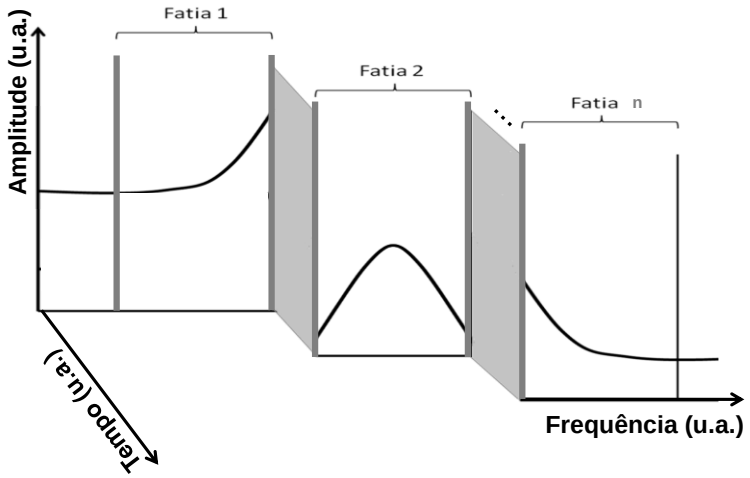

Figura 7 – Ilustração do efeito da técnica no espectro óptico.

Após a transmissão do sinal pela TON, o mesmo é recebido pelo elemento decodificador de sinais anteriormente ilustrado na Figura 6. O sinal é então, novamente, dividido nas *n* fatias espectrais, por meio de acopladores ópticos combinados com filtros. Os elementos contidos no decodificador, conforme ilustrados na Figura 6 são então ajustados para decodificar o sinal. Para esta decodificação, a *i-ésima* fatia deverá ser submetida a uma atenuação α_{max} - α_i e a um atraso τ_{max} - τ_i. É importante notar que, neste trabalho, as operações envolvendo as operações de α_i estão sempre expressas em dB. Assim, após o último acoplador, o sinal original será recuperado. Para medir a qualidade do sinal após a detecção é usada a taxa de erros de bit após a decodificação, BER_D. Neste trabalho convencionou-se que BER_D deve ser inferior a 1.10^{-12} para que o sinal possa ser considerado livre de erros. É importante notar que a decodificação do sinal transmitido utilizando a técnica proposta só será possível se o decodificador conhecer:

1. O número de fatias espectrais;
2. A largura de banda de cada fatia espectral;
3. A frequência central de cada filtro;
4. O perfil dos filtros;
5. A atenuação aplicada a cada fatia espectral;
6. O atraso aplicado a cada fatia espectral.

Quando propagado por uma TON, o sinal codificado passará por amplificadores ópticos. Estes dispositivos só provêm ganho a sinais com potência superior a um dado valor, P_{min}. Portanto, é imprescindível que a potência média do sinal codificado e α_{max} sejam ajustadas para garantir que, mesmo após todas as perdas até a entrada de cada amplificador na rota da TON, a fatia espectral com menor potência ainda tenha potência maior que P_{min}.

Também ao longo da propagação por uma TON, o sinal codificado estará sujeito a variações de potência impostas, por exemplo, por flutuações de ganho dos amplificadores. Neste trabalho, pressupõe-se que estas flutuações são idênticas para todas as fatias espectrais e, portanto, não afetam o desempenho da técnica. Tal suposição parece válida ao se notar que, no melhor de nosso conhecimento, tais flutuações não distorcem os sinais convencionais (isto é, sem codificação) que se propagam por TONs.

3.2 SINCRONISMO DAS CHAVES CRIPTOGRÁFICAS ENTRE CODIFICADOR E DECODIFICADOR

Pressupõe-se neste trabalho que ambos os extremos da TON detêm o conhecimento da chave aplicada e por esse motivo as pontas do canal da TON podem estabelecer a comunicação, como em outras técnicas existentes (TANENBAUM, 2003; CORNEJO, 2007). Na técnica proposta, é possível que a chave criptográfica possa ser alterada de maneira dinâmica. Nas subseções seguintes serão discutidas algumas maneiras para se manter o sincronismo das chaves criptográficas entre o codificador e o decodificador.

3.2.1 SINCRONISMO POR RELÓGIO

Uma possibilidade é que ambos os lados tenham em posse um arquivo que os diga qual a chave criptográfica será aplicada a cada momento. A partir desta biblioteca de chaves, o transmissor e o receptor utilizariam um sincronismo fornecido por um relógio e com base neste sincronismo ambos os lados saberiam qual a chave criptográfica a ser ajustada.

3.2.2 CHAVE COMPARTILHADA

Uma alternativa à proposta de sincronismo por relógio seria o próprio sistema fornecer o sincronismo. Para tal, o transmissor seria o responsável por determinar qual chave criptográfica será utilizada. Este processo pode ser feito de diversas formas, tais como:

- Ambos, transmissor e receptor, estariam ligados por um enlace dedicado de fibra para fornecer a chave do sistema. Este canal pode ser criptografado nas camadas superiores. Neste caso, o transmissor é o responsável por encaminhar a chave. Este procedimento está ilustrado na Figura 8.

- Ambos, transmissor e receptor estariam ligados a uma estação controladora das chaves criptográficas, e esta estação seria responsável por informar qual a chave que o sistema irá utilizar. Esta transmissão pode ser feita via enlaces de fibra óptica, sendo necessário o envio do horário de operação da chave criptográfica em conjunto com a própria chave. Este caso está ilustrado na Figura 9.

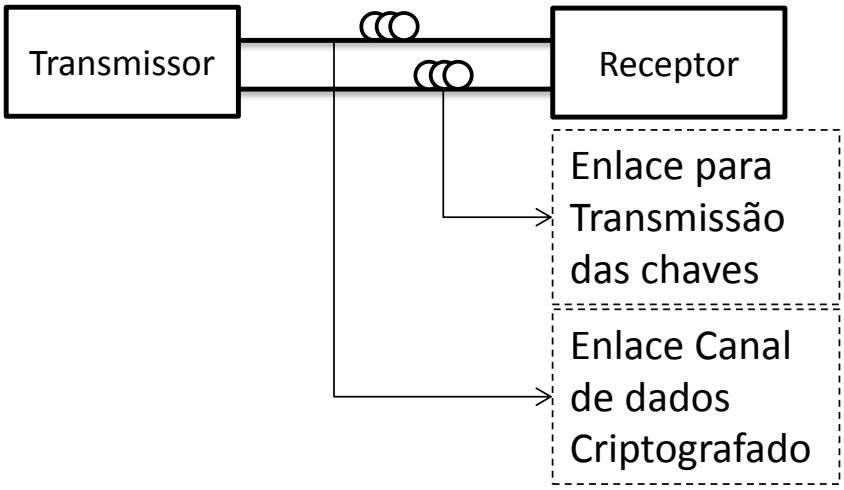

Figura 8 - Chave compartilhada pelo emissor.

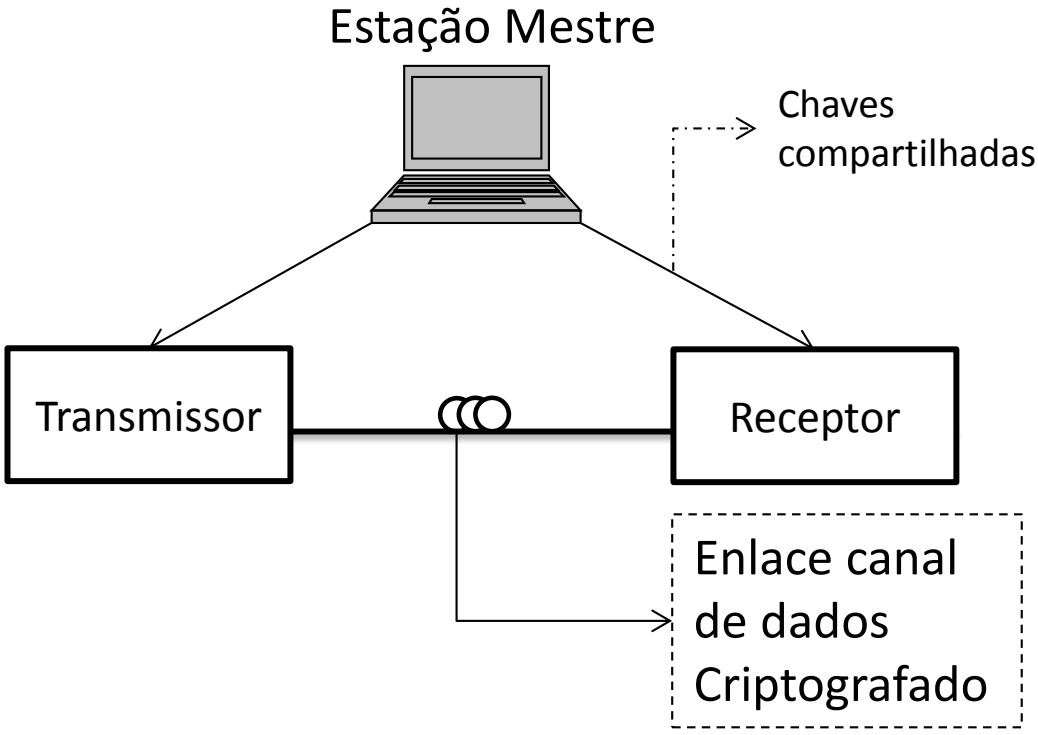

Figura 9 - Chave centralizada em uma estação mestre.

3.2.3 EQUIPAMENTO COMUTADOR DE CHAVES CRIPTOGRÁFICAS

Utilizando as técnicas apresentadas nas subseções anteriores, nas quais discutimos maneiras de prover o sincronismo de chave, a presente seção tem como objetivo discutir uma forma de realizar a comutação das chaves criptográficas. A técnica criptográfica proposta contempla diversas componentes na chave e mesmo com a implementação de métodos que permitam conhecer quais chaves serão utilizadas no sistema, o período de configuração do codificador e decodificador pode demandar um tempo considerável. Com o intuito de diminuir o tempo de troca de chaves, e por consequência diminuir uma parada forçada do canal, uma alternativa encontrada é a utilização de comutadores ópticos controlados eletronicamente.

Conhecendo antecipadamente qual a próxima chave e a hora em que a mesma começará a ser utilizada pela TON, uma posição do comutador no receptor do canal pode ser configurada a fim de estar preparado para decodificar o sinal. Cada seleção dentro do comutador representaria um conjunto de acopladores, atenuadores, retardadores de sinal e filtros que formariam a chave criptográfica, conforme mostrado na Figura 10.

Observa-se que a utilização de chaves dinâmicas aumentaria a complexidade e o custo dos codificadores e decodificados considerados. Apesar destas desvantagens a troca de chaves é essencial para impedir o sucesso de ataques realizados por agentes não autorizados.

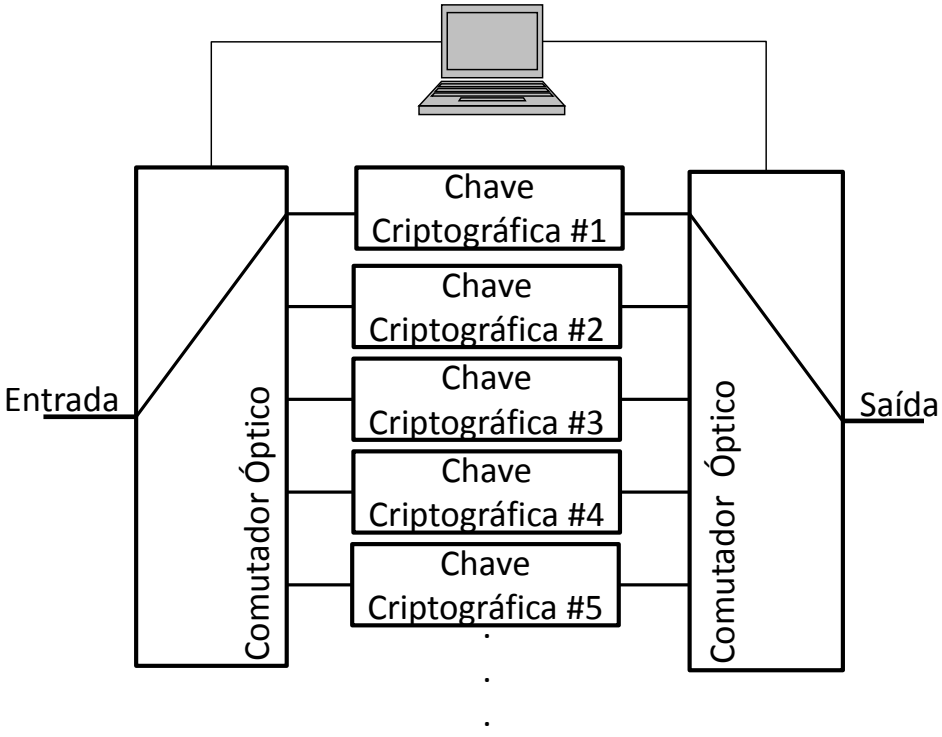

Figura 10 - Comutador das chaves criptográficas.

DESCRIÇÃO DAS SIMULAÇÕES

Neste capítulo descrevem-se as configurações utilizadas durante as diversas simulações realizadas neste trabalho. Na Seção 4.1 apresenta-se o arranjo inicial da simulação utilizando sistema *back-to-back*, ou seja, com o codificador conectado diretamente ao decodificador. Na Seção 4.2 descreve-se o arranjo da simulação para um sistema de transmissão de até 400 km.

4.1 ARRANJO PARA CONFIGURAÇÃO *BACK-TO-BACK*

A Figura 11 ilustra o diagrama de blocos relativo ao arranjo utilizado nas simulações que foram executadas com o *software* VPITransmissionMaker, versão 8.7, da VPIPhotonics Inc. Foram usados sinais com modulação NRZ-OOK ou DQPSK modulados por uma sequência pseudoaleatória de bits (*pseudo-random bit sequence*, PRBS) de 2048 bits e com potência de pico de 1 mW (0 dBm). Foi dado um ganho *G1* no amplificador, um amplificador à fibra dopada com Érbio (*Erbium doped fiber amplifier* - EDFA), para que a potência de pico do sinal na saída do codificador fosse mantida ~1 mW. O sinal foi transmitido pelo codificador (o qual recebe a chave criptográfica óptica descrita no capítulo anterior).

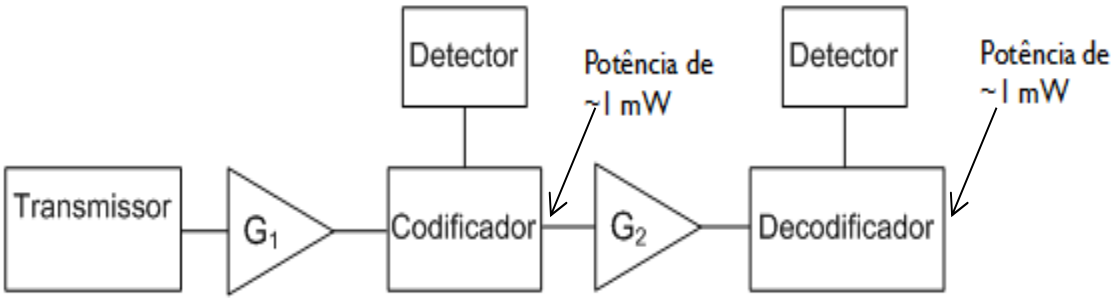

Figura 11 – Diagrama de Blocos do codificador e do decodificador.

No circuito do decodificador o sinal foi amplificado pelo amplificador *G2*, para compensar as perdas inerentes ao processo de decodificação, e para manter a potência de pico do sinal na saída do decodificador em ~1 mW. Após o ajuste da potência do sinal óptico, o mesmo foi transmitido pelo decodificador para que assim o sinal original fosse recuperado. Observa-se que com a potência de pico do sinal óptico ajustado para ~1 mW por *G1* e *G2*, a BER do sinal codificado e do sinal decodificado podem ser comparadas após a fotodetecção do sinal óptico. Para o cálculo de BER foi utilizado a aproximação gaussiana descrita em (SCHWARTZ, 1966; VPIPHOTONICS, 2011). Outras configurações do *software* VPITransmissionMaker, versão 8.7 utilizadas para avaliar a BER estão indicadas no Apêndice A.

A fim de compreender como os parâmetros α_i e τ_i influenciam o desempenho da técnica com um número tratável de variáveis, na maioria dos casos, foram analisadas apenas três fatias espectrais. Para modulação NRZ-OOK e DQPSK foi considerada uma taxa de transferência de bits de 40 Gbit/s. Os filtros utilizados na técnica de criptografia por fatiamento espectral tiveram seu perfil modelado para representar equipamento de mercado. Foram utilizados filtros com largura de banda de 20 GHz e 40 GHz, e seus perfis foram modelados conforme equipamento da fabricante Yenista, modelo XTM-50 (ITU-T G.692). O perfil desses filtros está ilustrado na Figura 12.

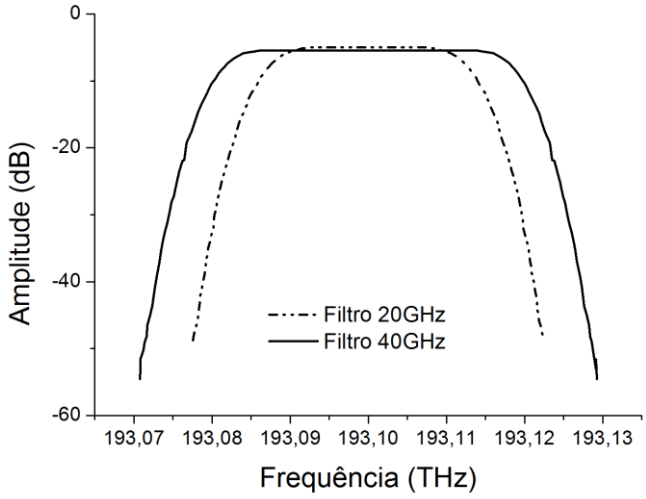

Figura 12 - Perfil dos filtros de 20 GHz e 40 GHz usados no trabalho.

Outras simulações foram executadas considerando a transmissão do sinal óptico em canais de transmissão WDM. Estas simulações foram realizadas a fim de verificar o efeito de transmissões na grade 50 GHz (ITU-T G.692) tanto em BER_C quanto em BER_D. Para esta simulação foram utilizados no codificador 3 fatias espectrais com filtros de 20 GHz de largura de banda, conforme ilustrado na Figura 13. Após o acoplamento, o sinal codificado foi transmitido por meio de um filtro de 50 GHz, gerando assim o sinal de acordo com a norma (ITU-T G.692). No decodificador foram utilizados 3 filtros de 20 GHz para recuperar o sinal codificado.

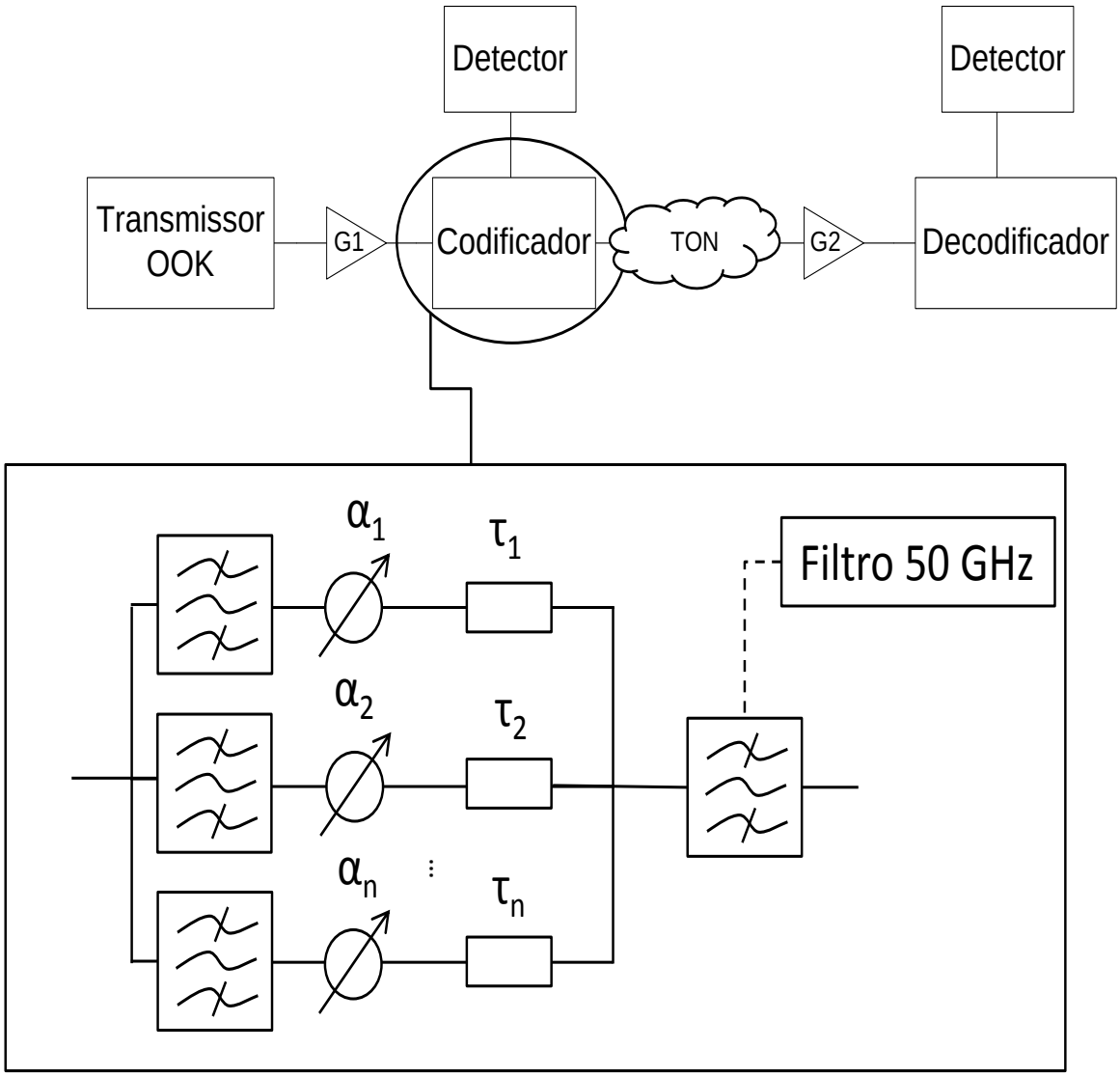

Figura 13 – Codificador adaptado para trabalhar na grade de 50 GHz.

4.2 SIMULAÇÃO EM SISTEMAS DE TRANSMISSÃO ATÉ 400 km

A Figura 14 ilustra o diagrama de blocos do arranjo utilizado para simular o comportamento da técnica em sistemas de transmissão em TONs. Nesta simulação foram utilizados enlaces com fibra padrão monomodo com comprimento, *l*, de 40 km, com coeficiente de dispersão igual a 16 ps/nm.km, inclinação de dispersão 80 ps/(nm^2.km) e atenuação de 0,2 dB/km. Além disso foram utilizadas fibras compensadoras de dispersão (*Dispersion Compensation Fiber - DCF*), com comprimento, l_{DCF}, de 7,11 km, com coeficiente de dispersão igual a -90 (ps/nm).km, inclinação de dispersão 80 ps/(nm^2.km) e atenuação de 0,6 dB/km. Estes parâmetros foram ajustados para que as DCFs compensassem exatamente a dispersão gerada pela fibra padrão. O sinal na saída do *i*-ésimo enlace foi amplificado por G2.*i*, a fim de compensar as perdas geradas pelo conjunto de fibras padrão e DCF.

É importante mencionar que as simulações basearam-se em um transmissor com largura de linha de 0 Hz. Porém, testes complementares com larguras de linha superiores a 10 MHz indicaram que os resultados obtidos não foram afetados pelo incremento deste parâmetro. Admitiu-se que o ganho dos amplificadores fosse suficiente para compensar as perdas de inserção nos elementos da simulação (filtros, atenuadores, compensadores de dispersão e

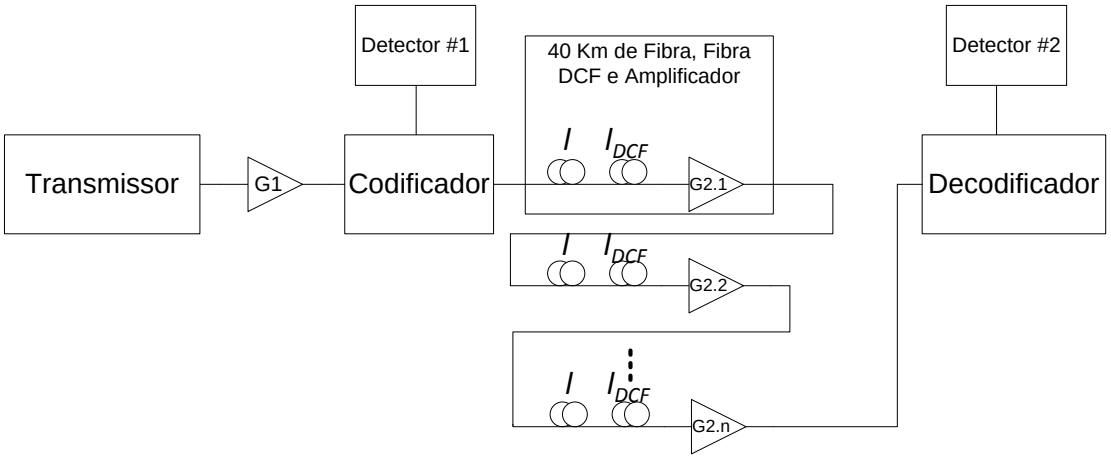

Figura 14 - Arranjo das simulações para sistemas de transmissão de até 400km.

outros). Outros parâmetros relevantes utilizados nas simulações estão apresentados no Apêndice A.

A dispersão de modo de polarização (*polarization mode dispersion*, PMD) é um efeito que afeta drasticamente o desempenho de sistemas de comunicação óptica com taxas iguais ou superiores a 10 Gbps, como os considerados neste trabalho (Breuer, 2003). Por se tratar de um efeito aleatório, a PMD é atualmente compensada eletronicamente a partir de módulos de processamento digital de sinais (*digital signal processing*, DSP) utilizados nos receptores (Bulow, 2008). Nas simulações realizadas neste trabalho não se considera a ação da PMD e admite-se que, assim como ocorre com os sinais não-codificados que trafegam pelas TONs, a compensação deste efeito é realizada a partir de módulos de DSP.

5 RESULTADOS

Neste capítulo abordam-se os resultados obtidos nas simulações utilizando a técnica criptográfica proposta para sinais NRZ-OOK e DQPSK a 40 Gbps. Na Seção 5.1 apresentam-se os resultados obtidos para a técnica utilizando a modulação NRZ-OOK e filtros de 40 GHz de largura de banda. Na Seção 5.2 apresentam-se os resultados relativos a filtros com essa mesma largura de banda e sinais com modulação DQPSK. Na Seção 5.3 apresentam-se os resultados para as modulações NRZ-OOK e DQPSK em sinais restritos à grade de 50 GHz do ITU-T.

Para verificar o comportamento da técnica proposta a BER do sinal codificado e a BER do sinal decodificado devem ser analisadas em conjunto. Em particular considera-se que a BER do sinal codificado, BER_C, é satisfatória quando supera o limite de 10%. De fato, como mencionado anteriormente, em sistemas binários a maior BER possível é de 50%.

Em situações *back-to-back*, a BER do sinal decodificado, BER_D, foi considerada satisfatória para valores inferiores a 10^{-12}. De fato, como em outros trabalhos (REIS Jr., 2009), sinais com BER abaixo deste limite estão livres de erros. Apesar de ser entendido que BERs abaixo de 10^{-12} dificilmente são medidas em sistemas práticos, muitas vezes, valores inferiores a este limite foram mostrados em nossos gráficos para ilustrar o comportamento da BER em função de algum parâmetro de interesse.

A BER limite após a propagação dos sinais por enlaces ópticos foi considerada como $1x10^{-12}$. No entanto, este valor poderia ser aumentado para

~ 10^{-3} caso técnica de correção posterior de erro (*forward error correction*, FEC) fosse considerada.

Observa-se que em muitas figuras apresentadas neste capitulo os valores de BER_C e BER_D são apresentadas no mesmo gráfico. O valor de BER_C é mostrado no eixo da esquerda e o valor de BER_D é mostrado no eixo da direita. Nota-se também que as unidades da atenuação α, do atraso τ e do espaçamento entre filtros Δf foram omitidas nas legendas dos gráficos, mas sempre correspondem, respectivamente, a dB, ps e GHz.

5.1 SINAL NRZ-OOK

Para a simulação foi utilizado um sinal NRZ-OOK de 40 Gbps, com uma PRBSde 2048 bits. A Figura 11 ilustra o arranjo da simulação para o sistema *back-to-back*, descrito no capítulo anterior. Nesta seção, considera-se que o sinal foi dividido em 3 fatias espectrais.

5.1.1 INFLUÊNCIA DA ATENUAÇÃO

Primeiramente o impacto da atenuação na fatia central, que contém a maior parte da informação, é analisado. A Figura 15 ilustra a BER do sinal codificado e a do sinal decodificado em função da atenuação na fatia central. Observa-se que a BER do sinal codificado é adequada (maior que 10%) para uma atenuação superior a 15 dB. Nota-se que valores significativos de BER do sinal codificado foram obtidos quando valores superiores a esta atenuação na fatia central foram utilizados. De fato, para atenuações próximas a 30 dB chegou-se a BER_C= 42 %, valor este muito próximo ao limite de 50%. No entanto, para α_2> 25 dB, $BER_D \leq 1.10^{-6}$. Assim apesar da técnica ser

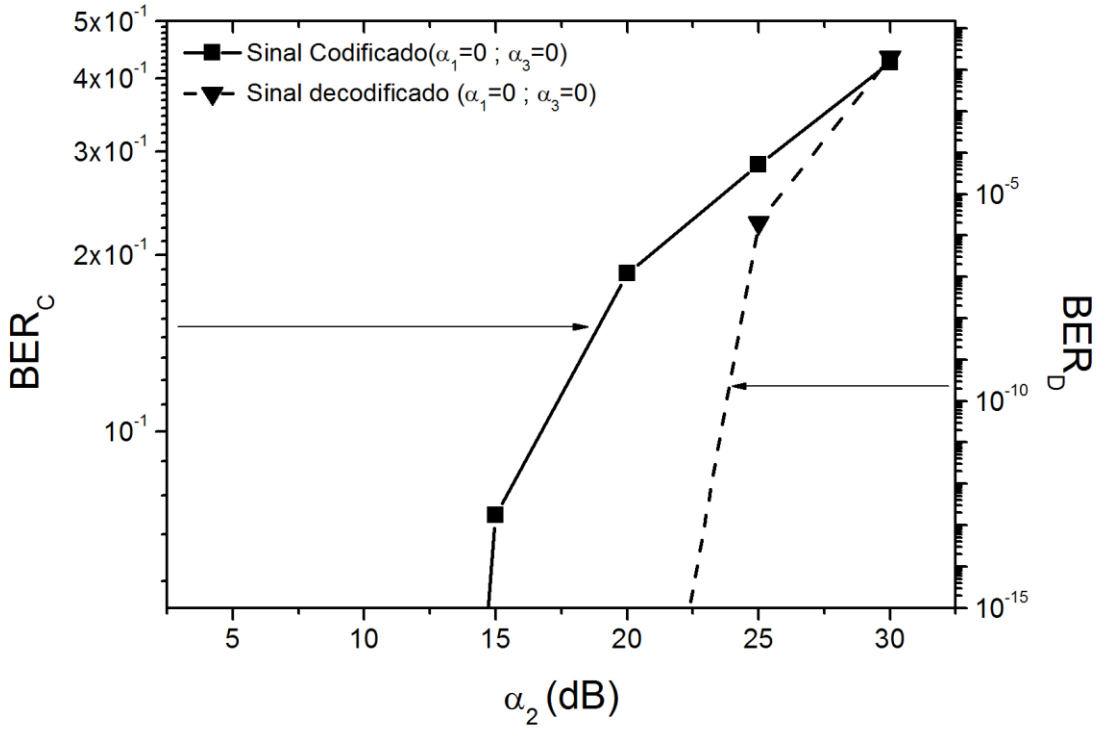

Figura 15 – *BER*$_C$ e *BER*$_D$ em função de α_2, com $\alpha_1 = \alpha_3 = 0$ dB.

satisfatória em termos de codificação do sinal ela não atingiu as métricas consideradas satisfatórias para a decodificação.

Também foi investigada a influência de α_1 sobre *BER*$_D$ e *BER*$_C$. Verificou-se que essas duas taxas de erro de bit mantiveram-se abaixo de 10^{-20}. Apesar de este resultado ser satisfatório do ponto de vista da decodificação do sinal, ele não é adequado com relação à codificação do mesmo. Dada a simetria relativa à primeira fatia, resultados e conclusões similares também foram obtidos para a influência de α_3 sobre *BER*$_D$ e *BER*$_C$. Observa-se que em condições experimentais reais seria extremamente difícil medir ou avaliar BERs da ordem de 10^{-20}. Por esta razão, não apresentamos em forma de gráfico os resultados descritos neste parágrafo.

Para todos os níveis de atenuação a técnica não se mostrou eficaz quando utilizada simultaneamente as bandas laterais como componentes da chave criptográfica. Neste caso, BER_C apresentou valores que são considerados livres de erros, abaixo de 10^{-20}, não atingindo a métrica estabelecida no trabalho e isto pode ser verificado na Figura 16. Neste caso, não encontramos nenhum intervalo no qual os valores de BER_C e BER_D sejam simultaneamente satisfatórios. Devido à dificuldade prática previamente mencionada em relação a medidas de BER inferiores a 10^{-20}, a curva para BER_C não é ilustrada no gráfico da Figura 16.

Conforme pode ser visto nas figuras anteriores desta seção, BER_C e BER_D não atingem simultaneamente os valores estabelecidos como adequados

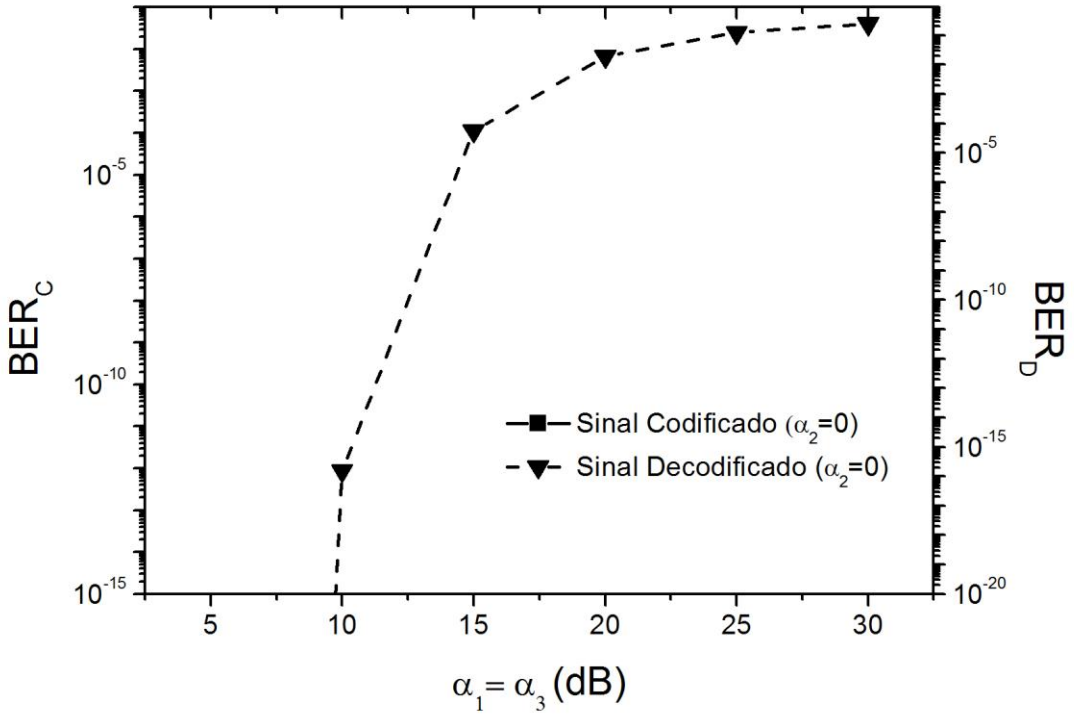

Figura 16 – BER_C e BER_D em função de α_1 e α_3, com α_2= 0 dB.

neste trabalho. De forma a encontrar uma solução para este problema, procurou-se variar o espaçamento, Δf, entre os filtros. Isto então permitiu reduzir a sobreposição de diferentes fatias espectrais. O espaçamento entre filtros, Δf, está ilustrado na Figura 17. Uma abordagem mais detalhada do impacto do uso do espaçamento entre filtros está descrita na Seção 5.1.4.

Para esta análise utilizou-se como exemplo a chave criptográfica com α_1= 0 dB, α_2= 25 dB e α_3= 0 dB. Segundo os resultados apresentados na Figura 15 esta configuração de chave implica em BER_D= 2,03x10^{-6}, para Δf= 40 GHz. A Figura 18 apresenta os resultados para uma varredura no intervalo de Δf= 45,0 a 45,8 GHz com incrementos de 0,1 GHz. Pode-se notar que o incremento de Δf causou uma melhoria significativa da BER_D. Os resultados obtidos chegaram ao valor desejado neste trabalho, que é de $BER_D < 10^{-12}$, quando utilizado um espaçamento entre filtros de 45,8 GHz.

A Figura 19 ilustra os resultados obtidos em função de Δf para a chave criptográfica α_1= 0 dB, α_2= 30 dB e α_3= 0 dB. Pode-se notar com este resultado uma melhora significativa nos resultados da BER_D quando Δf é aumentado.

Figura 17 – Representação do espaço entre filtros.

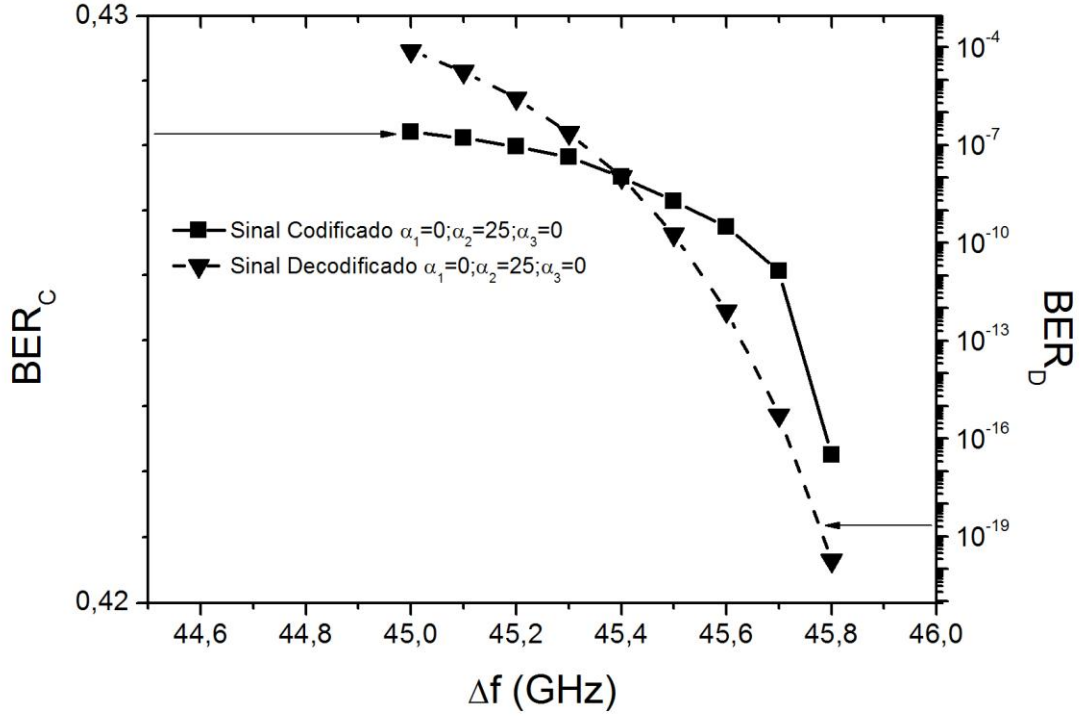

Figura 18 - *BER$_C$* e *BER$_D$* em função de Δf, com α_1= α_3= 0 dB e α_2= 25 dB.

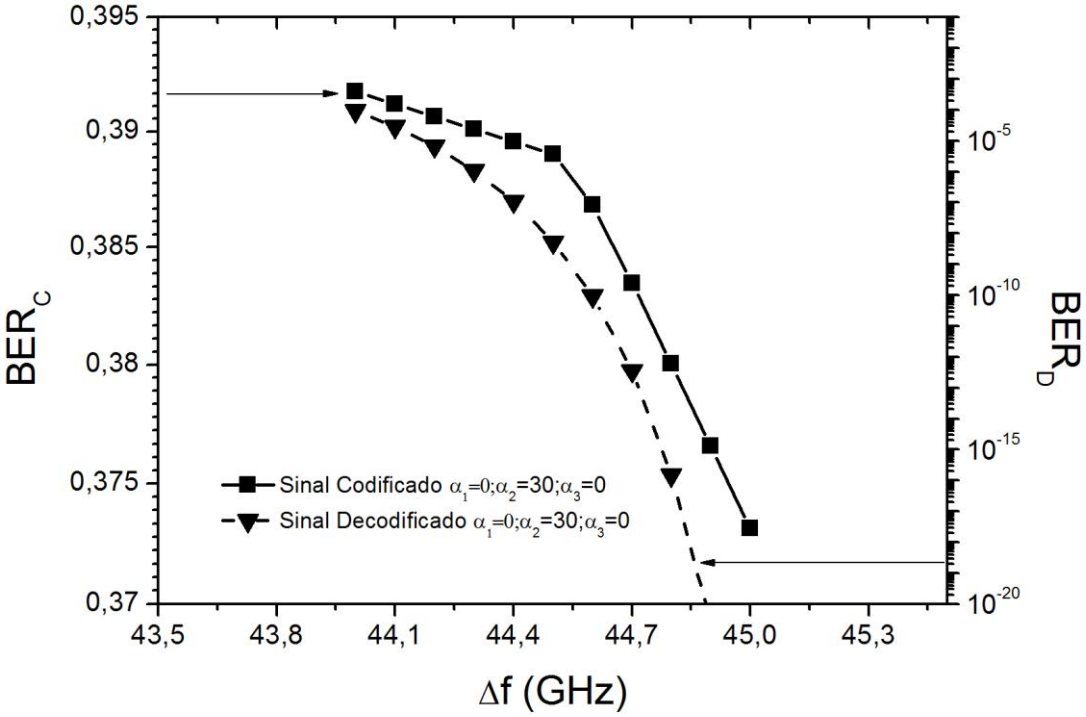

Figura 19 - *BER$_C$* e *BER$_D$* em função de Δf, com α_1= α_3= 0 dB e α_2= 30 dB.

Também é interessante analisar que para a Figura 18 e para a Figura 19 a diminuição dos valores de BER_D é contínua com o incremento em Δf. Como será mostrado na Subseção 5.1.4, isto é uma consequência da função de transferência relacionada ao conjunto do codificador e do decodificador.

Foram encontrados valores de Δf capazes de satisfazer o nível de BER desejado tanto no sinal codificado quanto no sinal decodificado. Isto pode ser visualizado na Figura 20, na qual os valores de Δf estão mostrados logo acima dos pontos do gráfico. Nota-se que a curva para BER_D não é ilustrada no gráfico desta figura porque os valores desta variável estão abaixo de 10^{-20}.

De forma a ilustrar o comportamento da técnica no diagrama de olho do sinal NRZ-OOK determinados valores de α_1, α_2 e α_3 foram utilizados. Na Figura

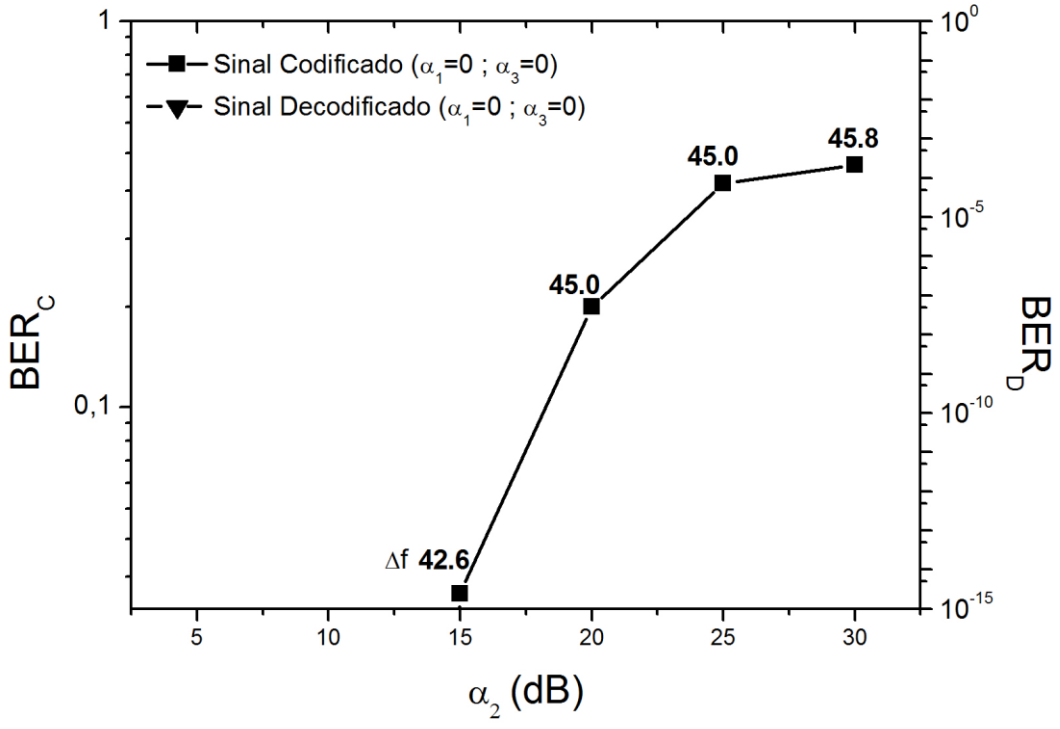

Figura 20 – BER_C e BER_D em função de α_2, com α_1= α_3= 0 dB.

21 (a) mostra-se o diagrama de olho do sinal elétrico aplicado na entrada do codificador. Aplicando uma chave que foi composta de α_1=5 dB α_2=25 dB α_3=0 dB, obtem-se o sinal na saída do codificador conforme mostrado na Figura 21 (b), e apresentando uma BER_C de 41,6% considerado ininteligível por qualquer receptor. Após a decodificação do sinal foi obtido um diagrama de mostrado na Figura 21 (c), considerado interpretável e livre de erros.

Verifica-se que nos resultados obtidos, a técnica começa a ser eficaz com o uso de atenuações, α_1, superiores a 15 dB na fatia central, e dependendo do valor de Δf utilizado. Com o uso de atenuação superior a 20 dB na fatia central BER_C avaliada apresenta valores superiores a 10%, atingindo, assim, a métrica proposta. Valores superiores a 33% são obtidos quando aplicada uma atenuação maior que 25 dB. Em todos os casos acima mencionados, a BER_D avaliada no decodificador foi inferior a 10^{-15}, e, portanto,

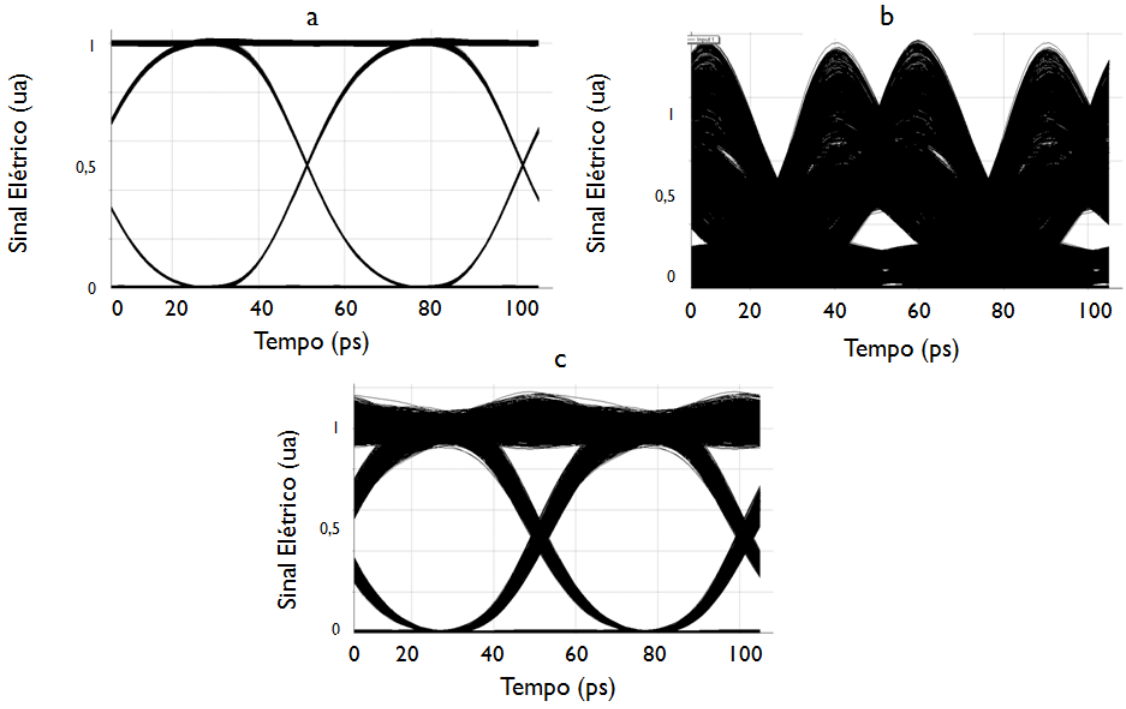

Figura 21 – Diagrama de olho na entrada (a), codificado com α_1=5 dB, α_2=25 dB e α_3=0 dB (b), e decodificado (c).

consideradas livres de erros.

Uma importante análise é o fato de além da atenuação empregada na chave é necessário também aplicar um valor de Δf para obter valores razoáveis de BER_D. Esta variável, bem como a atenuação, pode ser considerada parte integrante da chave criptográfica. Este fato pode ser comprovado uma vez que os resultados apresentados sem o uso deste artifício mostraram uma BER_D no decodificador inferiores a $2x10^{-2}$.

5.1.2 INFLUÊNCIA DO ATRASO

Primeiramente, analisou-se o impacto do atraso na primeira e na terceira fatias. O resultado pode ser observado na Figura 22, na qual foi aplicado atraso, τ_1, na primeira fatia, e na Figura 23, na qual foi aplicado atraso, τ_3, na terceira fatia. Verificou-se uma similaridade entre os resultados obtidos. Este fato ocorre devido à simetria entre as fatias 1 e 3. Valores de BER_C mostraram-se muito abaixo da métrica do trabalho e são, portanto, insuficientes para obtenção de um sinal codificado útil. Os valores de BER_D são satisfatórios e não estão apresentados na Figura 22 e na Figura 23 por serem menores que 10^{-20}.

Como teste adicional, foram aplicados diferentes níveis de atraso na fatia central. A Figura 24 ilustra a BER do sinal codificado e do sinal decodificado em função do atraso na fatia central. Novamente valores adequados de BER_D foram obtidos obedecendo, assim, os limites considerados. Apesar da melhoria da BER_C em relação à obtida quando utilizado τ_1 e τ_3 os resultados aplicando atraso na fatia central mostraram-se abaixo da métrica utilizada no trabalho.

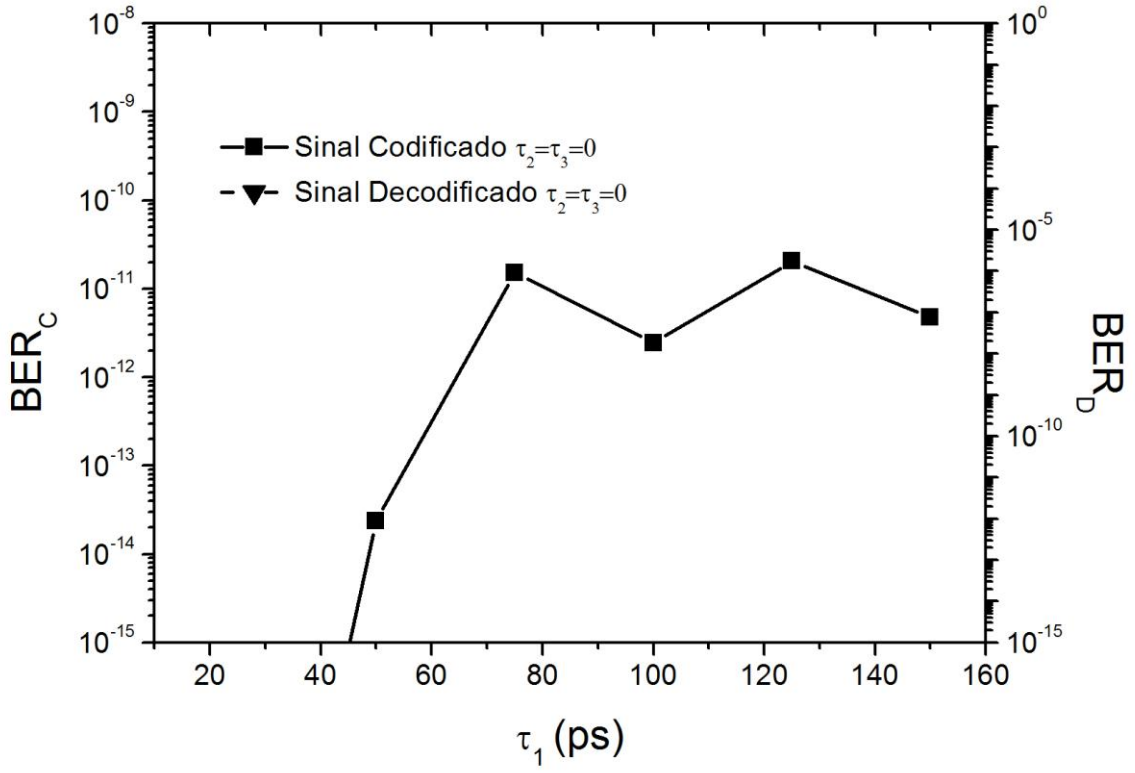

Figura 22 – *BER*$_C$ e *BER*$_D$ em função de τ_1, com τ_2= τ_3= 0 ps.

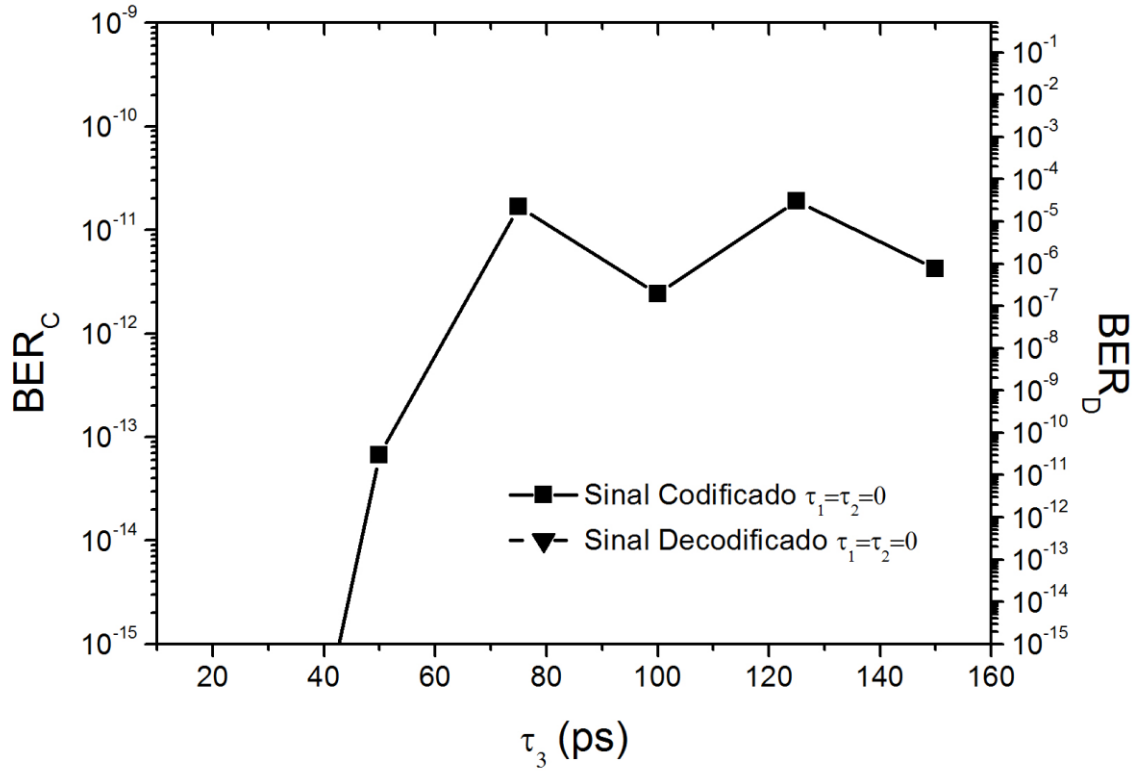

Figura 23 – *BER*$_C$ e da *BER*$_D$ em função de τ_3, com τ_1= τ_2= 0 ps.

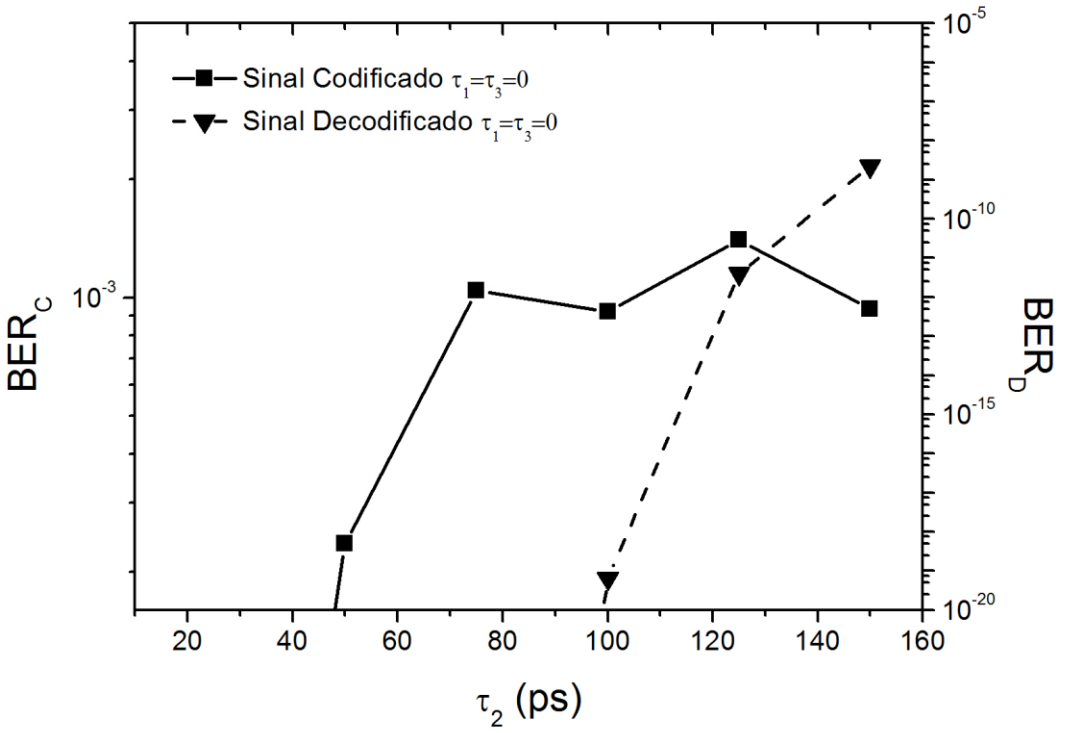

Figura 24 – BER_C e BER_D em função de τ_2, com τ_1= τ_3= 0 ps.

Conforme pode ser visto nas figuras anteriores desta seção, BER_C e BER_D não atingem valores considerados adequados para este trabalho. Uma solução para este fato, será apresentada na Subseção 5.1.4, na qual as influências do atraso e da atenuação são testadas simultaneamente.

5.1.3 INFLUÊNCIAS DA ATENUAÇÃO E ATRASO

Inicialmente analisou-se o impacto da utilização conjunta da atenuação e atraso na BER do sinal decodificado. Verificou-se que a inclusão do atraso na chave criptográfica conduziu a taxa de erro de bit do sinal decodificado a valores que são, na maioria dos casos, superiores a 10^{-12}. A fim de melhorar o desempenho da técnica, optou-se por introduzir, apenas no decodificador, um

atraso adicional, τ_a, à fatia espectral de maior energia (fatia central). Assim, o atraso considerado na fatia central do decodificador foi de (τ_{max}- τ_2)+ τ_a. A razão para a inclusão deste atraso adicional será apresentada na Seção 5.1.4.

A Figura 25 ilustra os resultados para uma chave com τ_1= τ_3= 0 ps, τ_2= 25 ps, α_1= 0 dB, α_3= 5 dB e α_2 variando entre 5 dB e 30 dB. Estes resultados foram obtidos a partir de uma escolha adequada de Δf e τ_a, estes valores estão indicados, respectivamente em GHz e ps no topo da figura. Observa-se que a BER do sinal codificado é adequada para uma atenuação superior a 15 dB. De fato, para atenuações próximas a 30 dB chegamos a BER_C de 37%, valor este muito superior à métrica usada no trabalho e muito próximo ao limite de 50%. Os valores de BER_D são inferiores a 10^{-12} para todas as atenuações $\alpha_2$consideradas. Isto indica um bom funcionamento da técnica quando o atraso adicional é incluído.

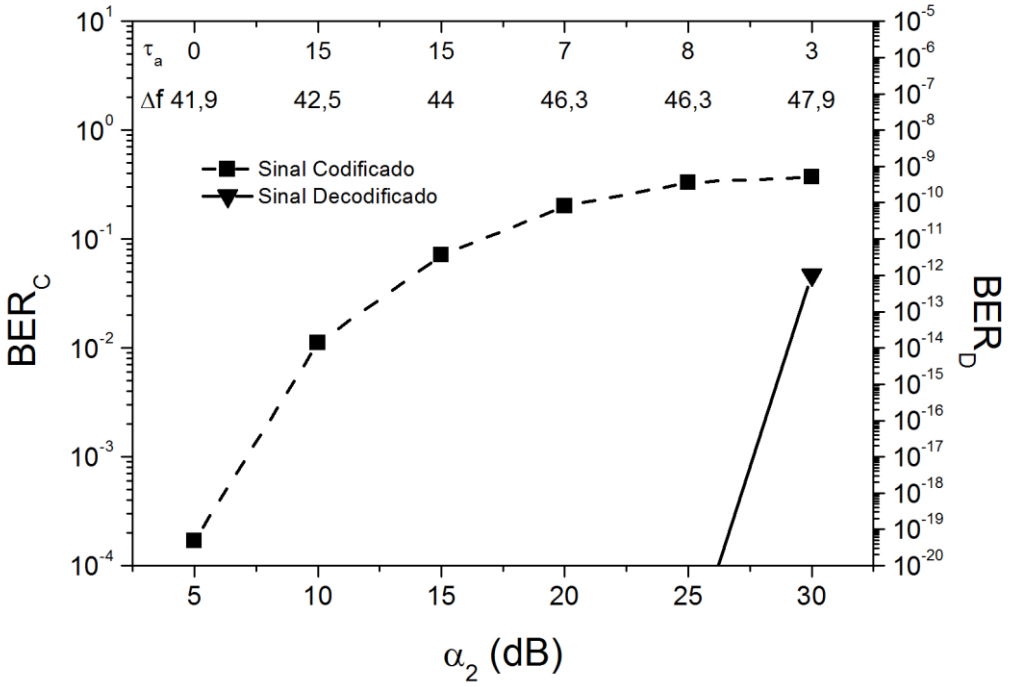

Figura 25 – BER_C e BER_D em função de α_2, com α_1= 0dB, α_3= 5 dB, τ_1= τ_2= 0 ps e τ_2= 25 ps.

Também foi analisado o desempenho da técnica para τ_2= 50 ps. O resultado pode ser observado na Figura 26. Estes resultados foram obtidos a partir de uma escolha adequada *de* Δf e τ_a, estes valores estão indicados, respectivamente em GHz e ps no topo da figura. Notam-se valores adequados de BER_C quando passamos a utilizar uma atenuação superior a 15 dB na fatia central. Valores de BER_D mostraram-se satisfatórios, isto é, $BER_D < 10^{-12}$ para $\alpha_2 \leq$ 25 dB. Assim o desempenho da técnica é adequado no intervalo 15 dB ≤ $\alpha_2 \leq$ 25 dB.

Os resultados das simulações não se mostraram satisfatórios em termos da BER do sinal decodificado quando utilizado valores de τ_2 superiores a 50 ps. A fim de encontrar uma alternativa para este fato o atraso τ_2 foi variado entre 25 ps e 50 ps com incremento de 1 ps. Obteve-se valores de BER_C e BER_D para todos os valores de τ_2 e os mesmos estão ilustrados na Figura 27. Os

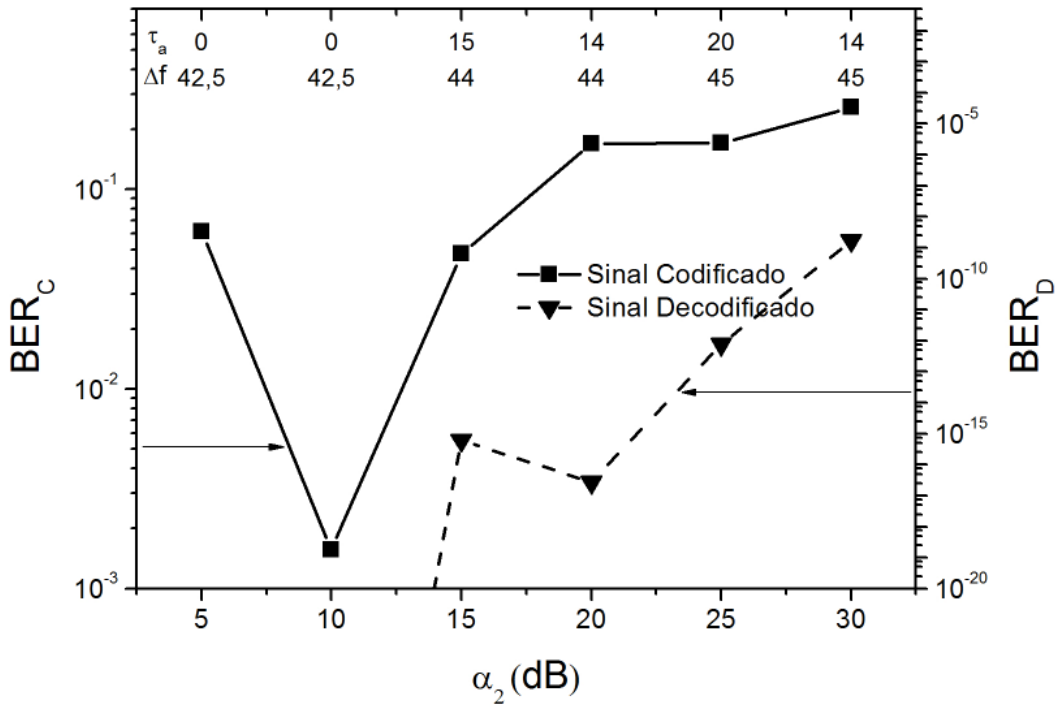

Figura 26 – BER_C e BER_D em função de α_2, com α_1= 0dB, α_3= 5 dB, τ_1= τ_2= 0 ps e τ_2= 50 ps.

valores de atenuação não foram variados e utilizou-se α_1=0 dB, α_2=20 dB e α_3=5 dB. Nestes testes, o atraso adicional τ_a foi variado entre 0 e 25 ps em incrementos de 1 ps, totalizando 625 simulações. Os valores de τ_a que proveram o menor valor de BER_D foram adotados e estão indicados no topo da figura. Os valores medidos de BER_C estão entre 18% e 33%, enquanto os valores de BER_D compreendem-se entre 10^{-2} a 10^{-41}. Nesta simulação constatou-se que dentre os 25 valores de atraso aplicados a τ_2, 6 valores de BER_D foram considerados satisfatórios, isto é, são inferiores a 10^{-12}.

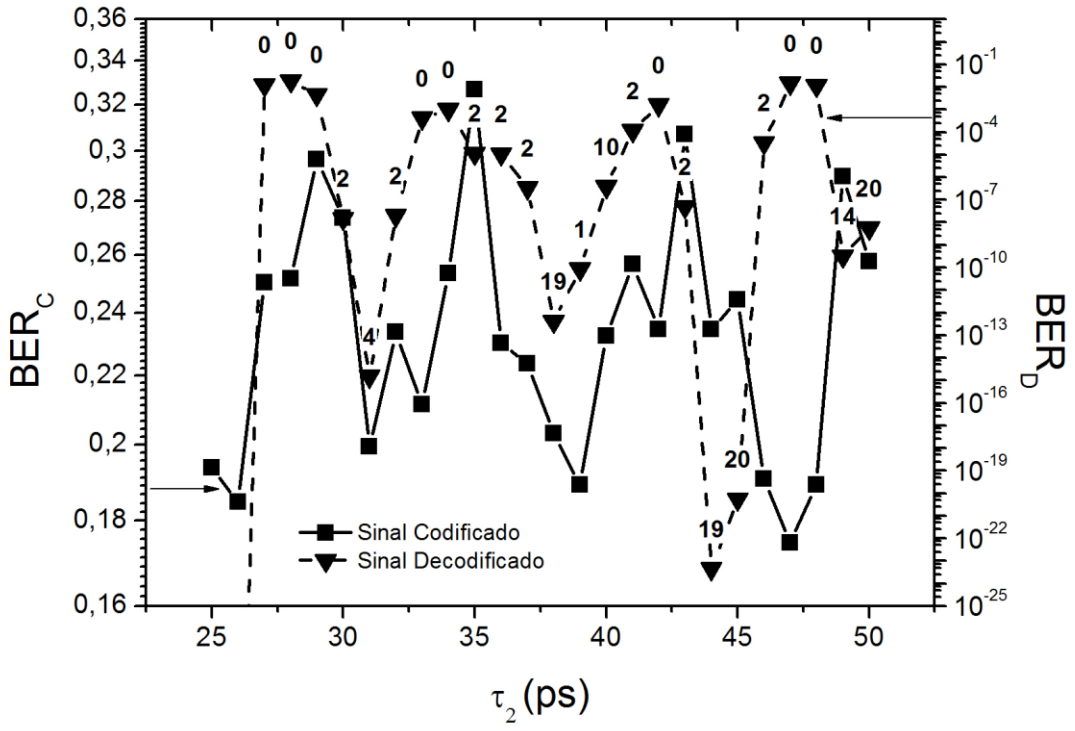

Figura 27 – BER_C e BER_D em função de τ_2, com α_1= 0 dB, α_2= 20 dB, α_3= 5 dB, τ_1= τ_2= 0 ps e Δf= 45 GHz.

5.1.4 JUSTIFICATIVA PARA VARIAÇÃO DO ESPAÇAMENTO ENTRE FILTROS E PARA UTILIZAÇÃO DE ATRASO ADICIONAL

Nas Seções 5.1.2 e 5.1.3 foram apresentadas as necessidades de se variar o espaçamento entre filtros, Δf, e adicionar um atraso, τ_a, para obter valores adequados de BER_C e BER_D. A fim de explicar a necessidade de utilizar estes dois parâmetros, realizaram-se simulações considerando que o sinal na saída do decodificador corresponde ao sinal de entrada transmitido por uma função de transferência, $H(\omega)$, que é o produto das funções de transferência que caracterizam o codificador, $H_c(\omega)$, e o decodificador, $H_d(\omega)$. Idealmente, $H(\omega)$ deveria ter um perfil retangular de amplitude ao longo da banda do sinal, para que o sinal de entrada não experimentasse distorções.

A Figura 28 ilustra o espectro de amplitude de $H(\omega)$, $|H(\omega)|$, para Δf= (a) 43,9 GHz, (b) 47,9 GHz e (c) 51,9 GHz, utilizando 3 filtros de 40 GHz. Observa-se que $|H(\omega)|$ apresenta deformações em relação ao perfil ideal esperado. Isto ocorre devido ao fato de os filtros utilizados no codificador e no decodificador não possuírem um perfil ideal (Figura 12). Observa-se ainda que, dentre os 3 valores de Δf considerados $|H(\omega)|$ foi mais próximo da ideal para Δf= 47.9 GHz.

A deformação mencionada no parágrafo anterior causará uma distorção temporal, isto é, uma dispersão, nos pulsos que se propagarem pelo codificador e decodificador. A fim de ilustrar este fato simulou-se a propagação de um único bit pelo codificador e pelo decodificador. A Figura 29 ilustra este bit (a) na entrada do codificador e na saída do decodificador para Δf= (b) 43,9 GHz, (c) 47,9 GHz e (d) 51,9 GHz. Nota-se que em todos os casos o sinal sofreu certa distorção após ser transmitido pelo sistema de criptografia e que esta distorção é menor para Δf= 47,9 GHz (função de transferência mais plana Figura 28 (b)).

A discussão anterior mostra a necessidade de se utilizar um valor adequado de Δf. Para entender a necessidade de utilização da compensação de atraso, a Figura 30 mostra um sinal (a) na entrada do codificador e após o decodificador para τ_a= (b) 0 ps e (c) 3 ps, com Δf= 47,9 GHz. Verifica-se que ambos os sinais de saída estão distorcidos em relação ao sinal de entrada. Esta distorção é devida à dispersão discutida anteriormente e é menor para o caso em que τ_a= 3 ps. De fato, BER_D é respectivamente $9{,}9 \times 10^{-6}$ e $1{,}8 \times 10^{-13}$. Os valores de Δf e τ_a utilizados nestas simulações são relativos ao ponto com α_2= 30 dB da Figura 25.

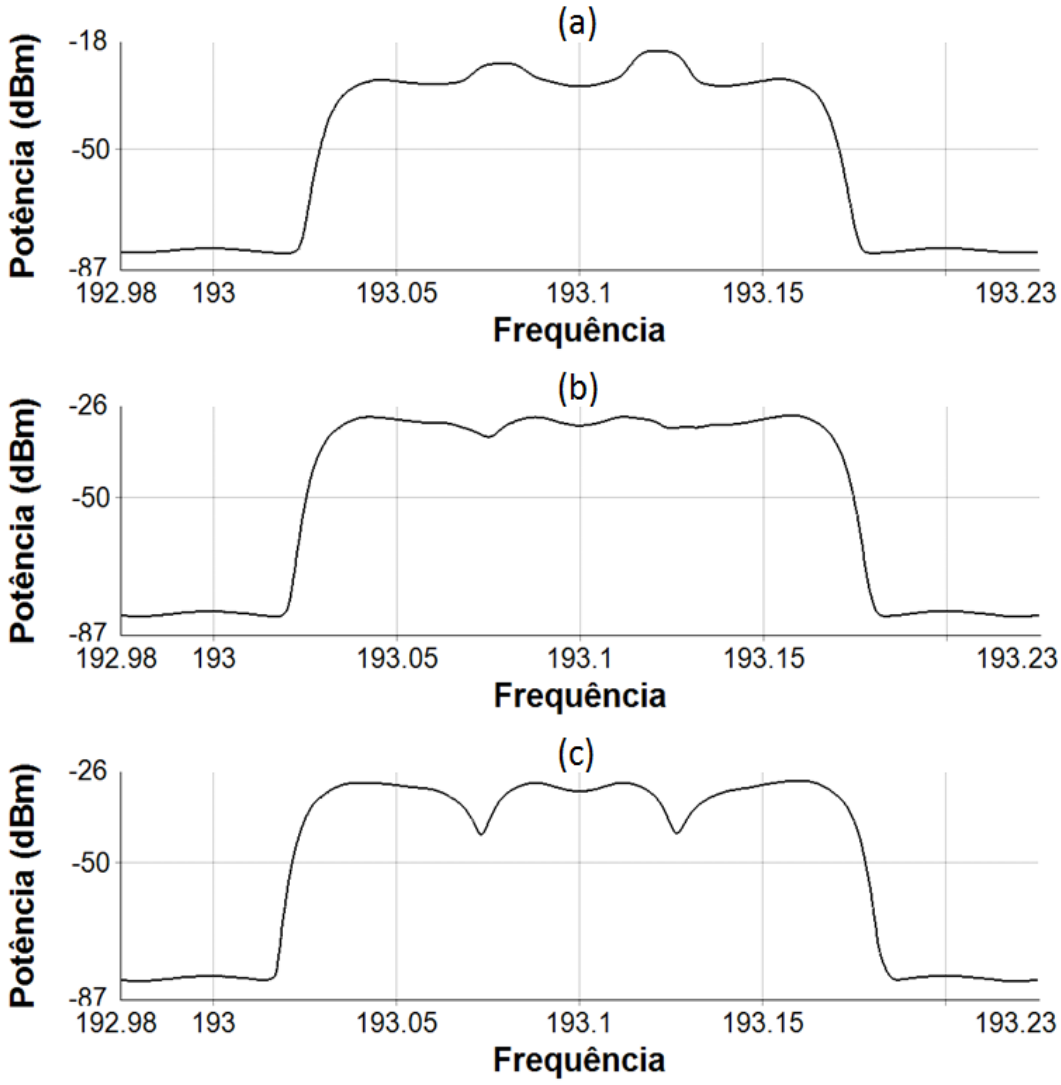

Figura 28 – Função de transferência do sistema com Δf= 43.9 GHz (a), Δf=47.9 GHz (b), Δf= 51.9 GHz (c).

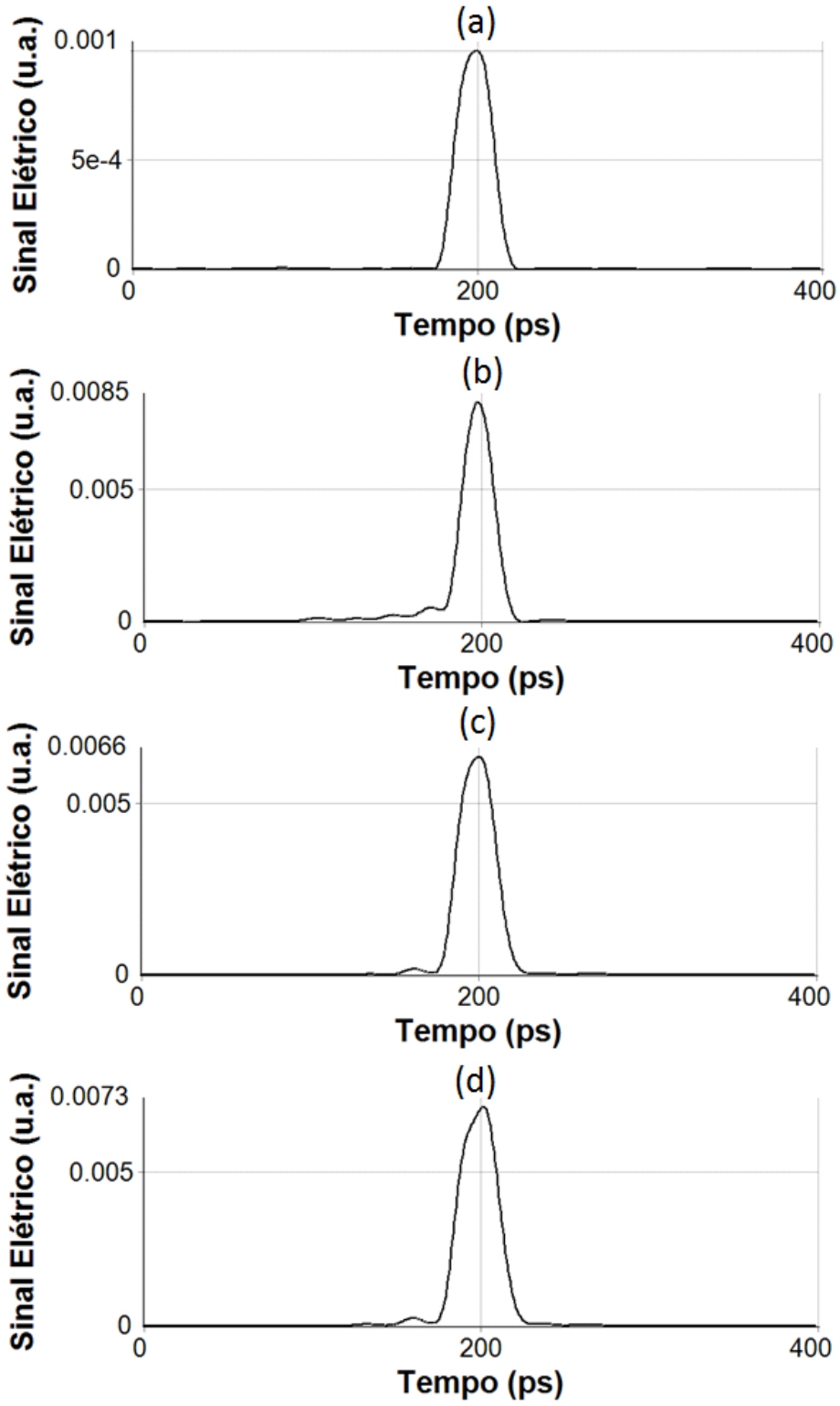

Figura 29 – Impacto da variação do Δf no bit com bit de entrada (a), Δf= 43.9 GHz (b), Δf= 47.9 GHz (c), Δf= 51.9 GHz (d).

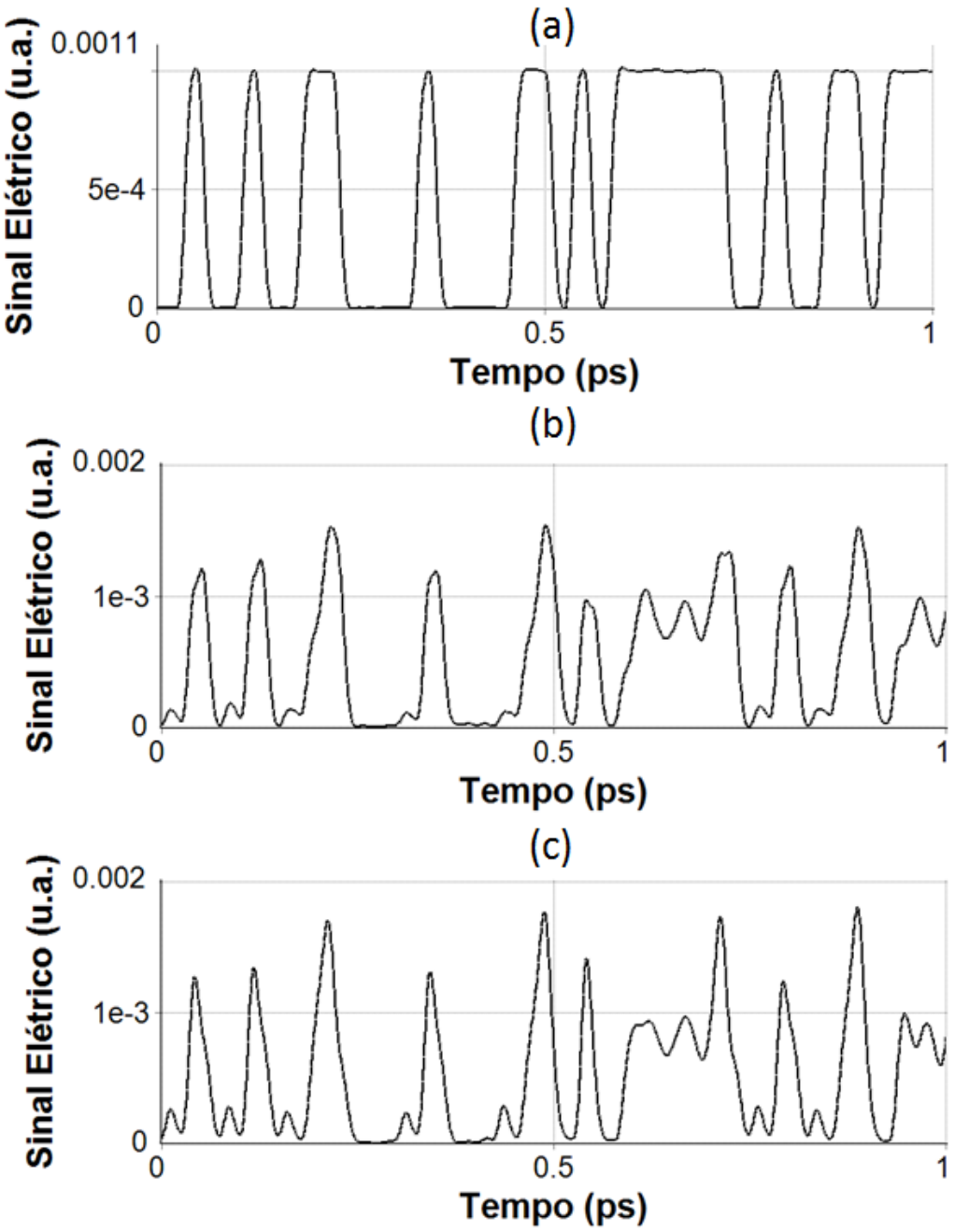

Figura 30 – Impacto da variação de τ_a no bit para a chave criptográfica α_1=0 dB, α_2= 25 dB, α_3= 5 dB, τ_1= 0 ps, τ_2= 25 ps, τ_3= 0 ps.

5.1.5 INFLUÊNCIA DA TÉCNICA EM TRANSMISSÕES ÓPTICAS

A fim de testar a eficácia da técnica em sistemas de transmissão óptica, um conjunto de chaves criptográficas foi usado para analisar o comportamento da técnica em um enlace óptico. Nesta simulação o sinal foi transmitido em enlaces de 40 km até atingir um máximo de 400 km. O efeito da transmissão na BER_C não foi considerado, tendo em vista que BER_C é avaliada logo após o codificador do sinal. Por este motivo esta taxa de erro de bit não sofre variação expressiva com o aumento do comprimento do enlace óptico. Os resultados mostraram-se satisfatórios para BER_D. De fato isto pode ser visto na Figura 31, na qual é apresentado o impacto do aumento do enlace na BER do sinal decodificado. Nota-se um impacto negativo na BER_D quando utilizado valor de α_2 igual a 25 dB, para distâncias até 280 km. Para os demais valores de α_2 os valores de BER_D atingiram a métrica estabelecida de até 10^{-12}.

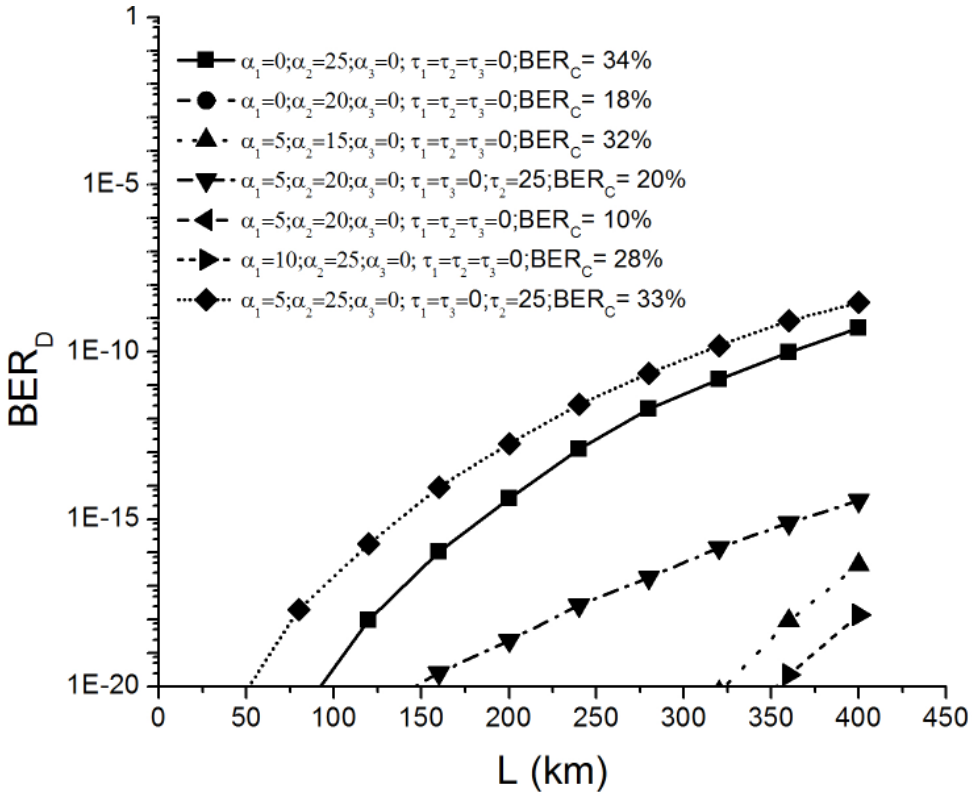

Figura 31 – BER_D em função da distância do enlace de transmissão para diversas combinações chaves criptográficas.

Importante notar que para os casos em que a diferença entre atenuações de α_1 e α_3 para α_2 não foi superior a 20 dB a variação da BER no decodificador foi mais expressiva. Este fato ocorreu mesmo quando utilizados valores de α_2 iguais a 25 dB, para este caso o valor de α_1 foi de 10 dB. Este fato ocorre devido do aumento da diferença de amplitude entre a faixa central e as faixas laterais, uma vez que a potência do sinal na fatia central é relativamente superior às demais fatias diminuindo, assim, a interferência sofrida pelas faixas laterais.

Também merece atenção o fato de que todos os valores, exceto os comentados acima, permitiram a transmissão do sinal por todo o caminho óptico, ou seja, pelos 400 km utilizados na simulação.

5.2 SINAL DQPSK

Na simulação desta seção foram utilizados sinais DQPSK de 40 Gbps, com uma sequência pseudoaleatória de bits (*pseudo-random bit sequence*, PRBS) de 2048 bits. A Figura 11 ilustra o arranjo da simulação para um sistema *back-to-back*, conforme descrito no capítulo anterior. Nesta seção, considera-se que o sinal foi dividido em 3 fatias espectrais.

5.2.1 INFLUÊNCIA DA ATENUAÇÃO

Primeiramente analisamos o impacto na atenuação na fatia central, que contém a maior parte da informação. A Figura 32 ilustra a BER do sinal codificado e a BER do sinal decodificado em função da atenuação da fatia central. Observa-se que a BER do sinal codificado é adequada para atenuações na fatia central maiores que 20 dB. Nota-se que valores

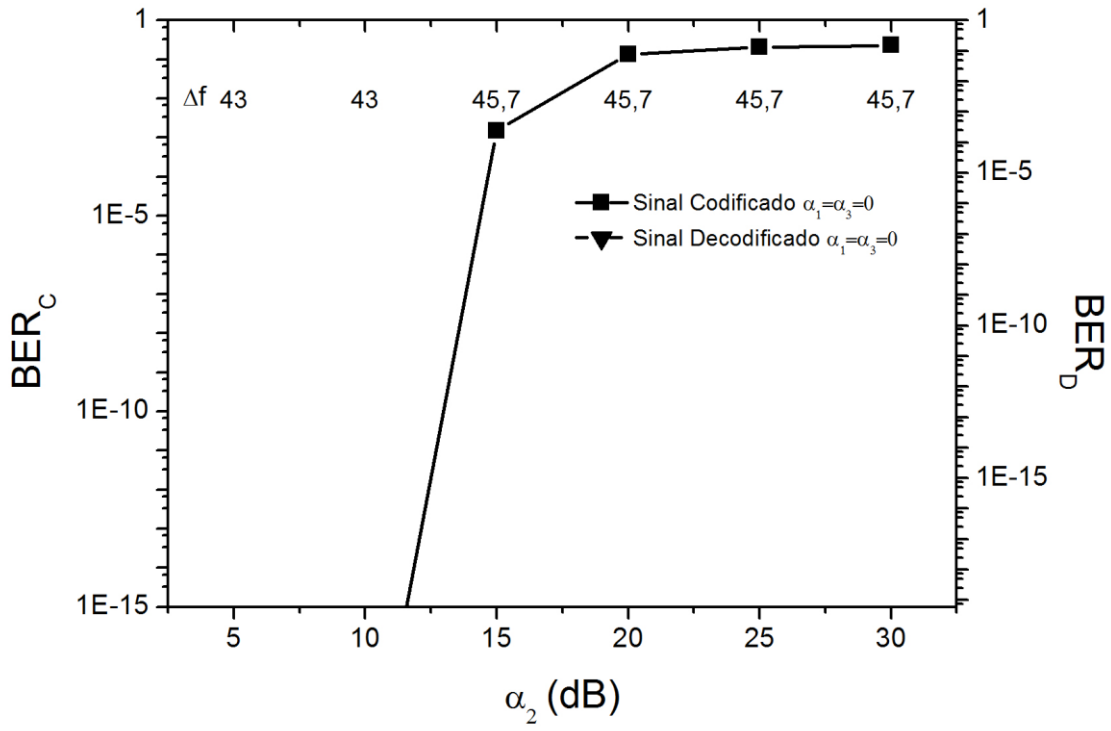

Figura 32 – *BER*$_C$ e *BER*$_D$ em função do incremento de α_2, combinado com α_1= α_3 = 0 dB, com os respectivos valores de Δf para cada valor de α_2.

significativos de BER do sinal codificado foram obtidos quando utilizados valores superiores a esta na fatia central. De fato, para atenuações próximas a 30 dB chegou-se a *BER*$_C$= 23%. Nota-se que a curva para *BER*$_D$ não é ilustrada no gráfico desta figura porque os valores desta variável estão abaixo de 10^{-20}. Assim como nos gráficos para o sinal NRZ-OOK, esta figura também indica o valor ótimo utilizado para Δf. Como visto nos resultados para sinais NRZ-OOK, os valores de *BER*$_C$ não se mostraram adequados quando usados α_1 e α_3 como chave única. Este fato foi reproduzido para o sinal DQPSK.

Como teste complementar foi adicionado um valor fixo de atenuação nas fatias laterais, em conjunto com a variação da atenuação da fatia central. O resultado pode ser observado na Figura 33, em que foi aplicada uma atenuação fixa na primeira fatia (α_1) e na Figura 34 em que foi aplicado uma atenuação fixa na terceira fatia (α_3). Verificou-se uma similaridade entre os

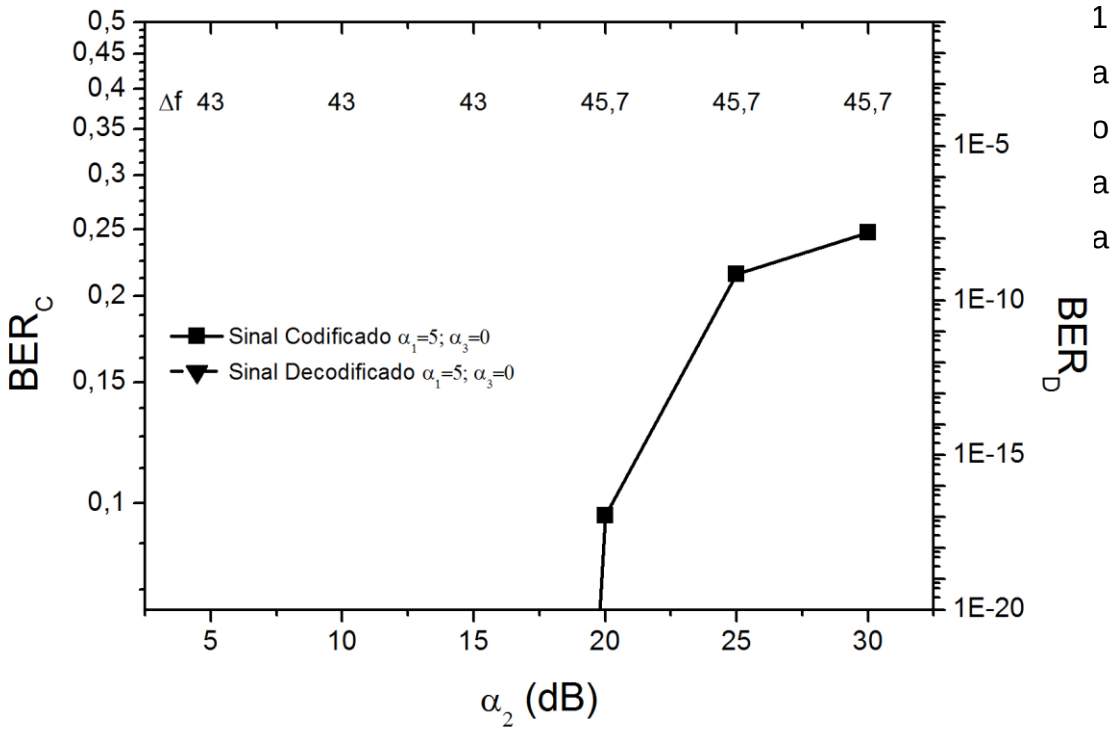

Figura 33 – *BER*$_C$ e *BER*$_D$ em função de α_2, com α_1= 5 dB e α_3 = 0 dB.

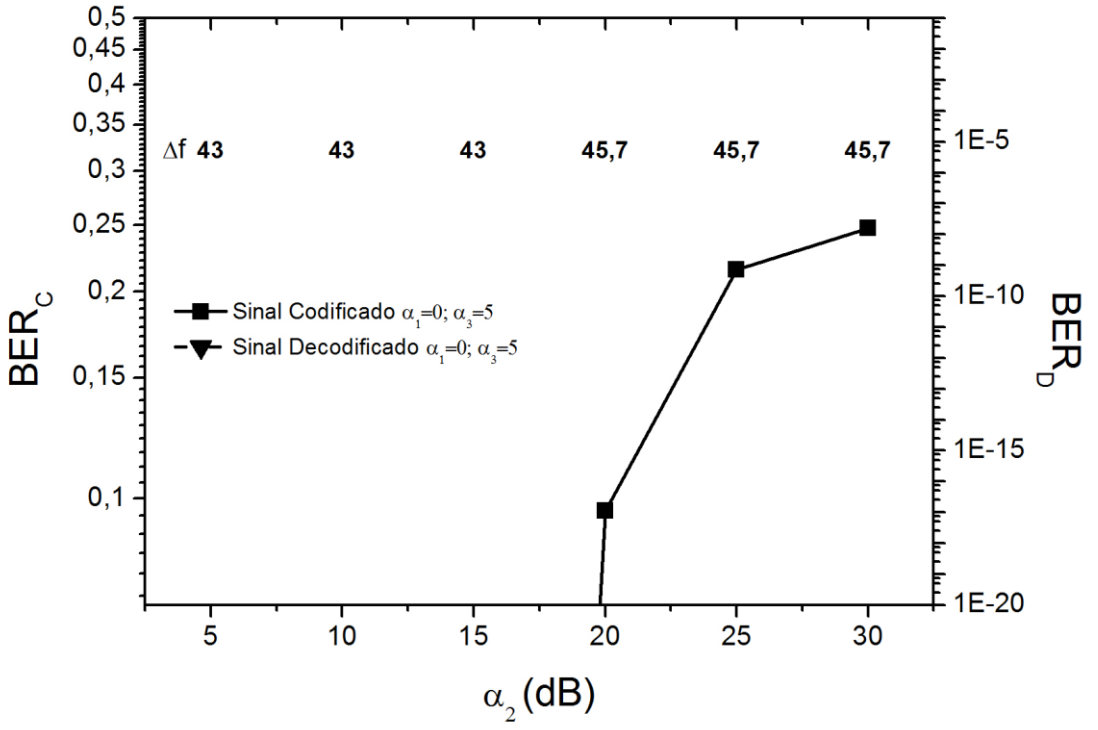

Figura 34 – *BER*$_C$ e *BER*$_D$ em função de α_2, combinado com α_1= 0 dB e α_3 = 5 dB.

De forma a ilustrar o comportamento da técnica no diagrama de olho do sinal DQPSK, valores de α_1, α_2 e α_3 foram escolhidos aleatoriamente. A Figura 35 mostra o diagrama de olho do sinal elétrico do canal 1 (primeiro dos canais binários que constituem o sinal) na entrada do codificador (a). Aplicando uma chave que foi composta de α_1=5 dB, α_2=25 dB e α_3=0 dB, obtivemos o sinal na saída do codificador conforme mostrado na Figura 35 (b), apresentando BER_D= 22%, considerado completamente inelegível por qualquer receptor. Após decodificação do sinal foi obtido um diagrama de olho conforme Figura 35 (c), considerado totalmente interpretável e livre de erros.

De forma complementar, a Figura 36 mostra o diagrama de olho do sinal elétrico canal 2 (o segundo dos canais binários que constitui o canal DQPSK) na entrada do codificador (a). Aplicando uma chave que foi composta de α_1=5 dB, α_2=25 dB e α_3=0 dB, obtivemos o sinal na saída do codificador conforme

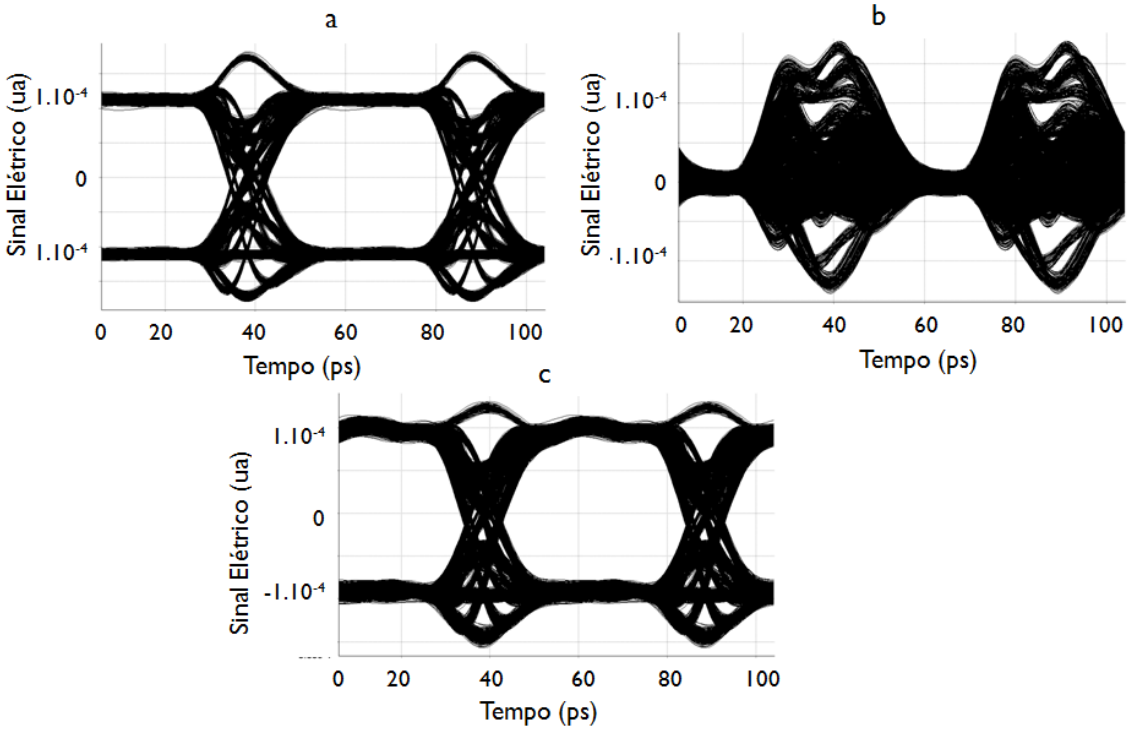

Figura 35 – Diagrama de olho na entrada (a), codificado com α_1=5 dB, α_2=25 dB α_3=0 dB (b) e decodificado (c) do canal 1 do sinal DQPSK.

mostrado na Figura 36 (b), e apresentando BER_D= 22% considerado ininteligível. Após a decodificação do sinal foi obtido um diagrama de olho conforme Figura 36 (c), considerado livre de erros.

Verifica-se que com os resultados obtidos, a técnica começa a ser eficaz com o uso de atenuações superiores a 20 dB na fatia central α_2. Da mesma forma que verificado nas seções anteriores, o uso de Δf foi essencial para obtenção dos resultados. Com o uso de atenuações superiores a 20 dB na fatia central a BER_C medida apresenta valores superiores a 10%, atingindo a métrica do trabalho. Para todos os casos acima mencionados BER_D apresentou valores inferiores a 10^{-15} e, portanto, pode ser considerado livre de erros.

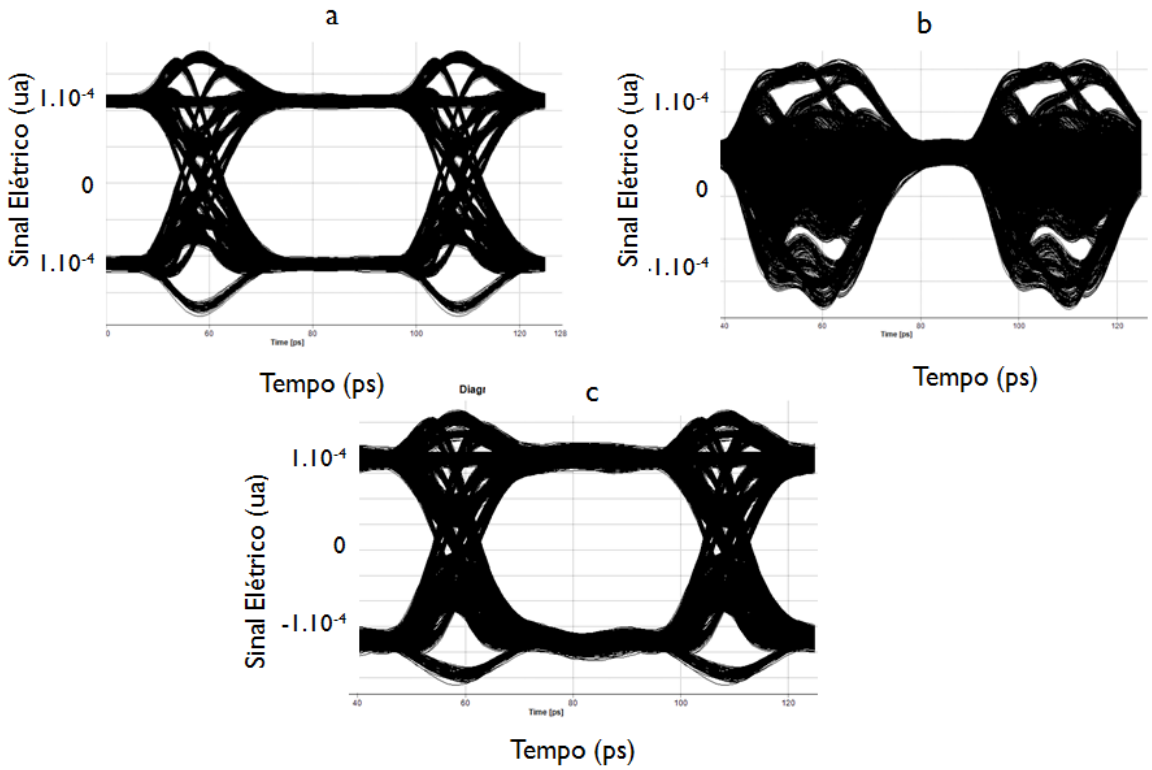

Figura 36 – Diagrama de olho na entrada (a), codificado com α_1=5 dB, α_2=25 dB e α_3=0 dB (b) e decodificado (c) do canal 2 do sinal DQPSK.

5.2.2 INFLUÊNCIA DO ATRASO

Primeiramente analisamos o impacto do atraso na segunda fatia. Aplicou-se um atraso entre 25 ps e 150 ps a primeira fatia, tanto BER_C quanto BER_D foram medidas < 10^{-15}, isto é, livres de erros. Apesar dos valores de BER_D sempre estarem abaixo da métrica do trabalho, os valores de BER_C mostraram-se muito abaixo da métrica do trabalho e, portanto, não suficientes para um sinal codificado prático. O mesmo resultado foi observado quando aplicado o atraso na primeira (τ_1) e na terceira (τ_3) fatias. Seus gráficos não são ilustrados devido ao fato que os valores medidos estão abaixo de 10^{-20}.

Verifica-se juntamente com os resultados obtidos na Seção 5.1.2 que o impacto do atraso na chave criptográfica é pouco significativo em termos de BER_C. Este fato pode ser explicado devido a relação de potência entre as bandas laterais e a banda central. Nota-se que a contribuição do atraso é pouco significativa, uma vez que a potência da banda central será sempre muito superior e suas componentes irão fazer com que o sinal seja sempre interpretado pelo receptor. Entretanto, resultados recentes mostram ao menos duas grandes vantagens na utilização do atraso (FOSSALUZZA JR., 2013). A primeira delas é que, quando os α_i são devidamente ajustados para prover BER_C da ordem de 10^{-3}, o atraso nas fatias espectrais pode ser adaptado para elevar esta taxa de erro de bit para valores superiores a 10%. A segunda vantagem é relativa ao embaralhamento temporal do sinal gerado. Tal efeito é extremamente desejável e diminui as chances de agentes não autorizados descobrirem a chave criptográfica utilizada por meio de ataques. Estas duas características ilustram a importância da utilização dos atrasos como parâmetro de criptografia.

5.2.3 INFLUÊNCIA DA ATENUAÇÃO E ATRASO

Primeiramente analisou-se o impacto da variação do atraso para determinadas chaves criptográficas. A Figura 37 ilustra os resultados de BER_C para as diversas combinações de chaves. Observa-se que os resultados de BER_C são adequados para atenuações superiores a 20 dB na fatia central, para todos os valores de τ_1. De fato com atrasos próximos a 150 ps, a BER_C apresenta valores de 30%.

Na Figura 38 observam-se os resultados obtidos para o decodificador. Os valores apresentados de BER_D apresentam-se adequados para a métrica do trabalho, com $BER_D < 10^{-12}$ para todos os valores de τ_1. De fato verifica-se que somente α_2= 20 dB apresenta $BER_D < 10^{-15}$ quando $\tau_1 > 100$ ps.

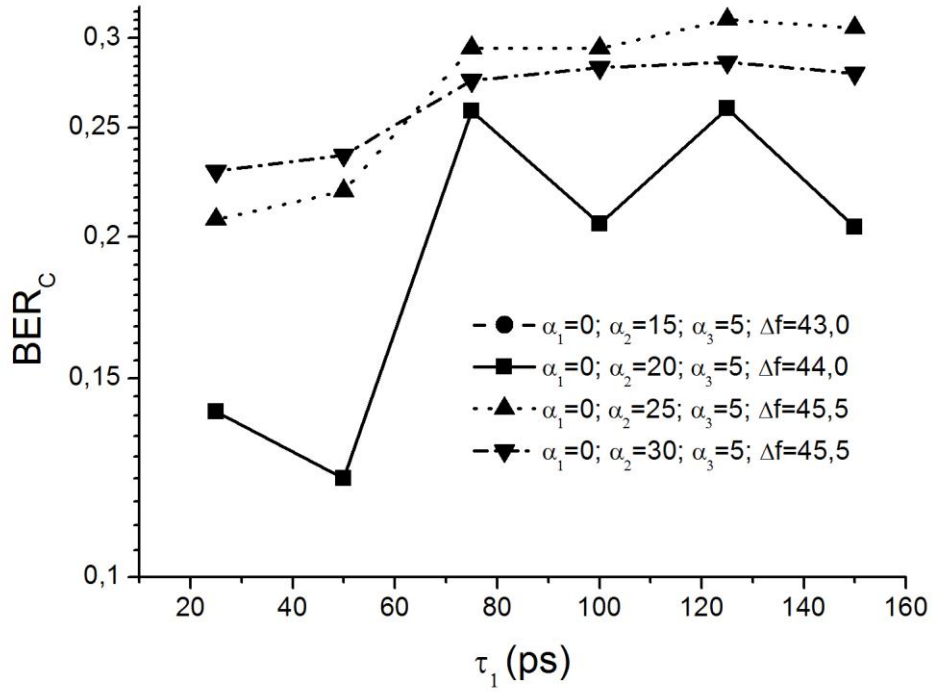

Figura 37 - BER_C em função de τ_1 para um conjunto de chaves criptográficas.

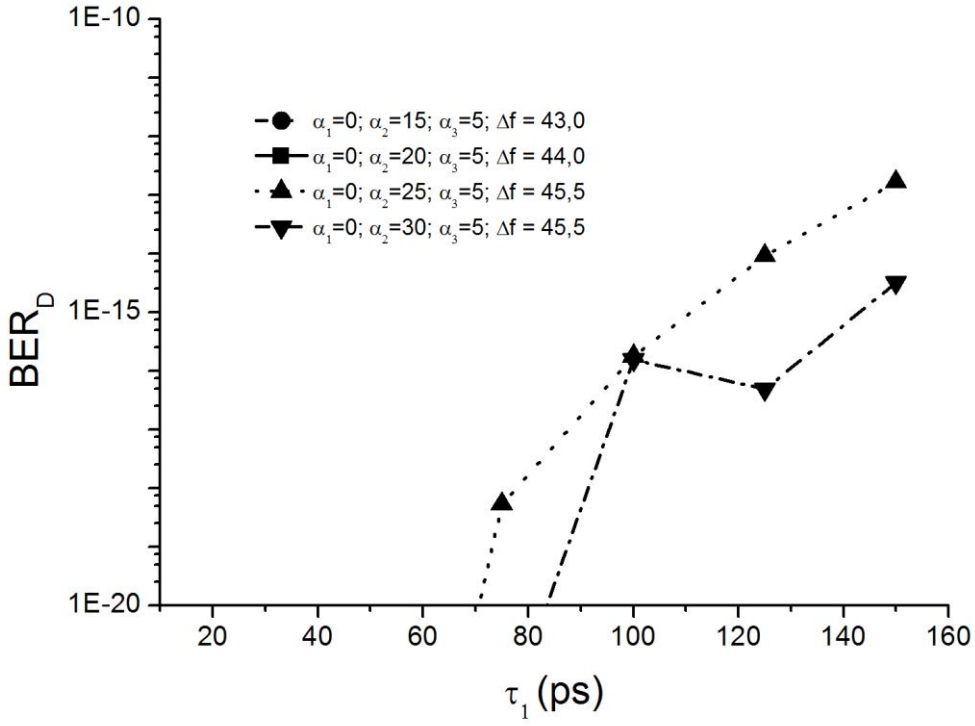

Figura 38 – BER_D em função do τ_1 para um conjunto de chaves criptográficas.

A seguir foram aplicados diferentes níveis de atraso na fatia central. A Figura 39 ilustra a BER do sinal codificado em função do atraso na fatia central para um conjunto de atenuações. Novamente, valores adequados de BER_C foram obtidos para todos os valores de α_2> 20 dB, obedecendo os limites considerados no trabalho. Em todos os resultados BER_D foi considerado satisfatório, isto é, abaixo da métrica.

Observa-se na Figura 40 os resultados obtidos para o sinal decodificado. Observa-se que os valores de BER_D foram satisfatórios para α_2= 15 dB e α_2= 20 dB, atendendo assim a métrica do trabalho para todos os valores de τ_2. Nota-se que BER_D para α_2= 25 dB foi considerada adequada somente para τ_2=25 ps. Verifica-se que somente α_2= 20 dB atendeu aos valores de BER_C e BER_D estipulados no trabalho para todos os valores de τ_2.

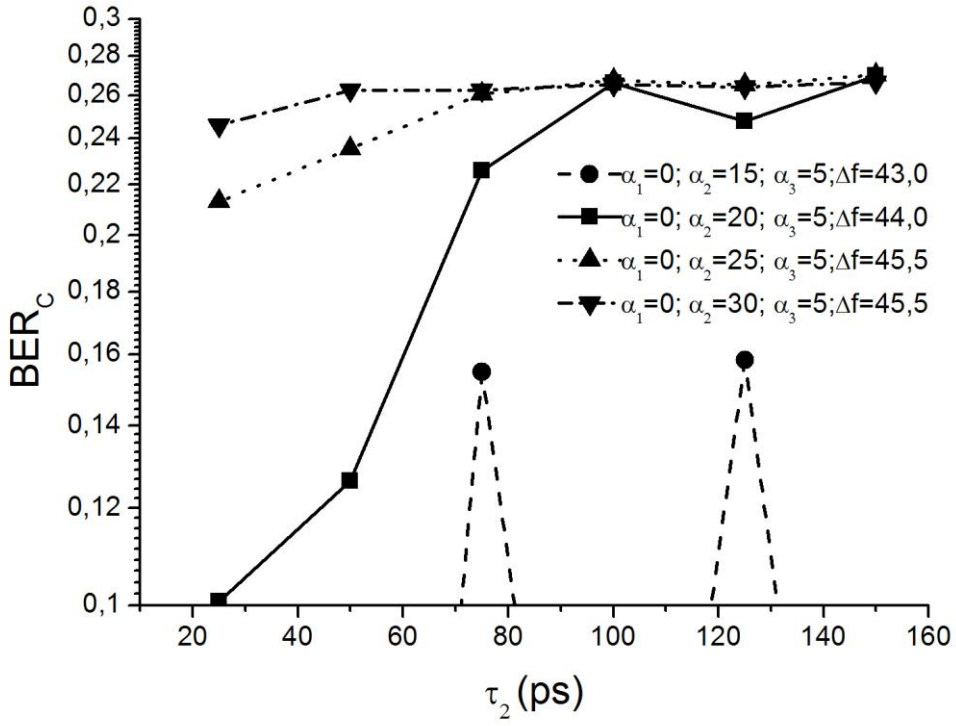

Figura 39 - *BER*$_C$ em função de τ_2 para um conjunto de chaves criptográficas.

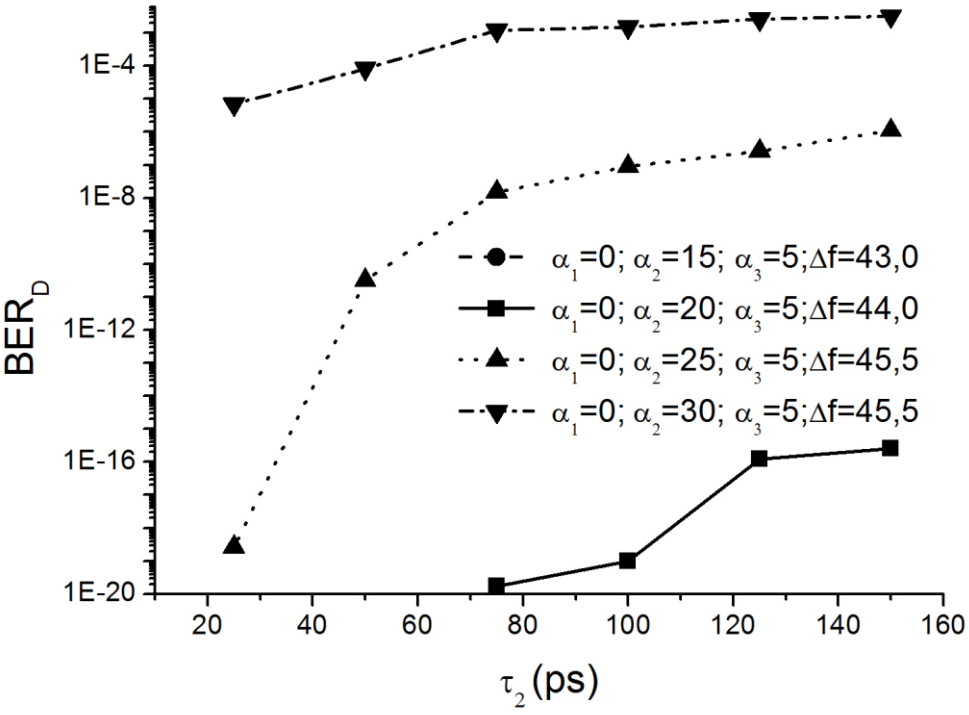

Figura 40 - *BER*$_C$ em função de τ_2 para um conjunto de chaves criptográficas.

Em uma análise complementar foram aplicados diferentes níveis de atraso na terceira fatia. Na Figura 41 ilustramos o impacto do uso da terceira fatia em BER_C. Valores adequados de BER_C foram obtidos quando α_2> 25 dB. Para α_2= 20 dB valores de BER_C foram adequados para τ_3= 75 ps e τ_3= 125 ps.

Na Figura 42 ilustramos o impacto do uso do atraso na terceira fatia na BER do sinal decodificado. Observa-se que a BER do sinal decodificado é considerada adequada para $\alpha_2 \leq$ 25 dB. Nota-se que para α_2= 30 dB a BER do sinal decodificado foi menor que o estabelecido no trabalho para τ_3= 25 ps. Importante notarmos que para este caso os valores de atenuação e atraso devem ser escolhidos criteriosamente para possibilitar o uso da técnica.

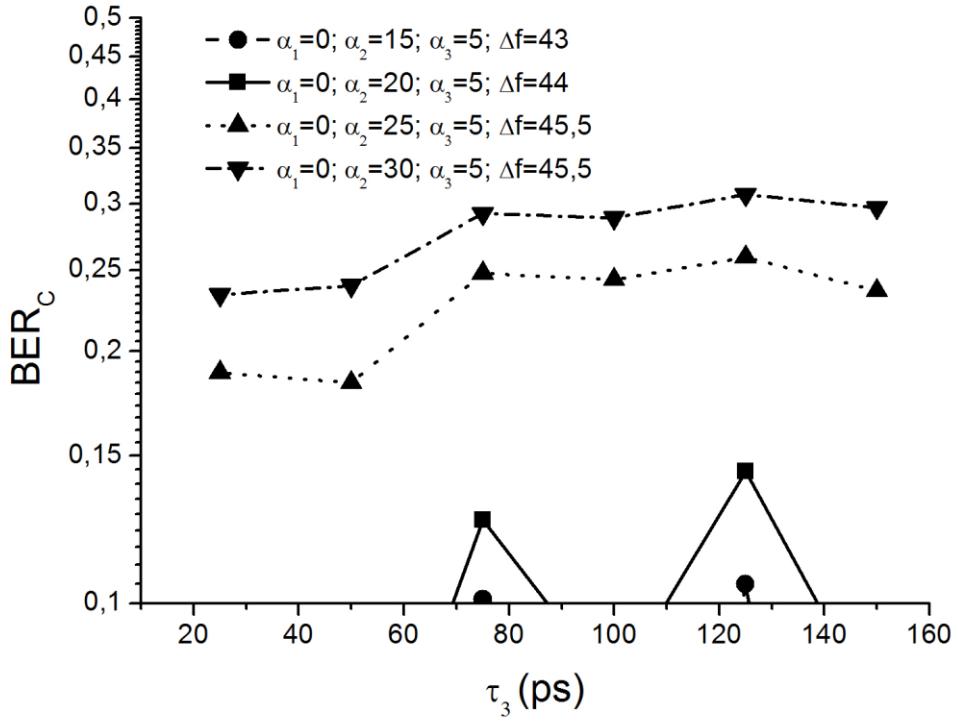

Figura 41 - BER_C em função de τ_3 para um conjunto de chaves criptográficas.

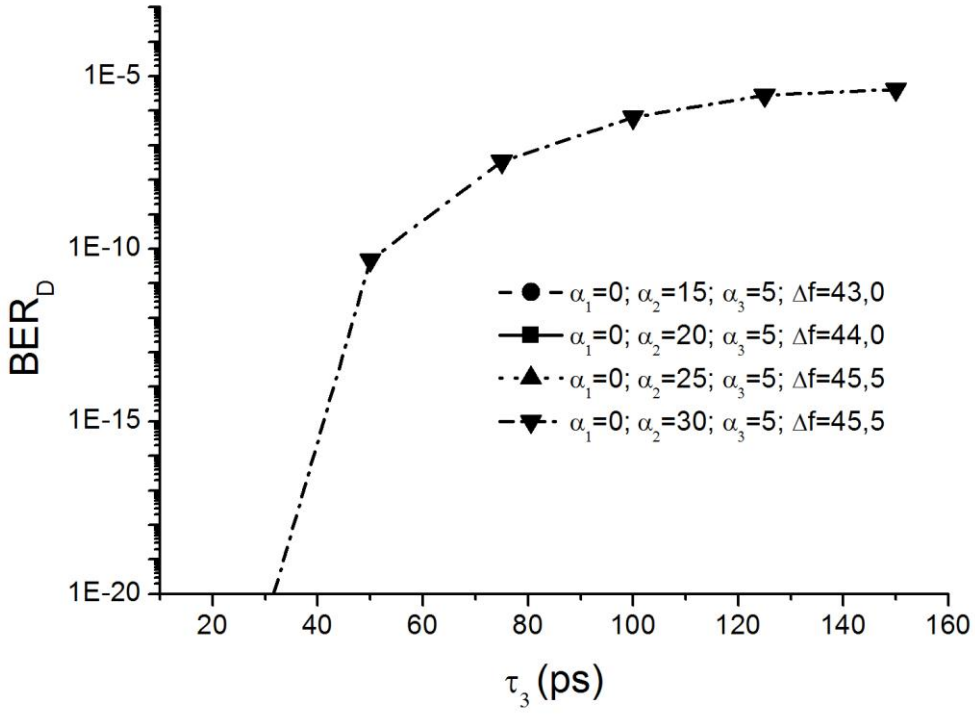

Figura 42 - BER_C em função de τ_3 para um conjunto de chaves criptográficas.

Conforme apresentado nesta seção verifica-se uma maior estabilidade nos níveis da BER do sinal codificado quando utilizado τ_1. Conforme ilustrado na Figura 37 a BER do sinal codificado ficou acima de 10% para valores de α_2> 15 dB, ao contrário do que ocorre na Figura 39 e Figura 41, que apresentam mais pontos abaixo dos 10%. Nota-se também que quando utilizado o atraso nas fatias que não contem atenuação (Figura 37), maior é a chance de que o sinal possa ser decodificado pelo receptor. Fato este ilustrado quando comparado os resultados entre Figura 37, Figura 39 e Figura 41.

5.2.4 PROPAGAÇÃO DE SINAIS ÓPTICOS

A fim de testar a eficácia da técnica em sistemas de transmissão óptica com modulação DQPSK, um conjunto de chaves criptográficas foram usadas para analisar o comportamento da técnica em um *enlace* óptico. Nesta

simulação o sinal foi transmitido em lances de 40 km até atingir um valor máximo de *enlace* de 400 km. O efeito da transmissão na BER_C não foi considerado, tendo em vista que a medição da BER é feita logo após o codificador do sinal. Por este motivo a BER no codificador não sofre variação com o aumento do comprimento do enlace óptico. Os resultados de BER_D mostraram-se satisfatórios para valores de α_2< 25 dB. De fato, isto pode ser visto na Figura 43, na qual é apresentado o impacto do aumento do enlace na BER do sinal decodificado. Nota-se um impacto negativo na BER_D quando utilizado valor de α_2 igual a 25 dB, para distâncias até 200 km. Para os demais valores de α_2 os valores de BER_D atingiram a métrica estabelecida de até 10^{-12}. Também merece atenção o fato que a maioria das configurações, permitiram a transmissão do sinal por todo o caminho óptico, ou seja, pelos 400 km utilizados no simulação.

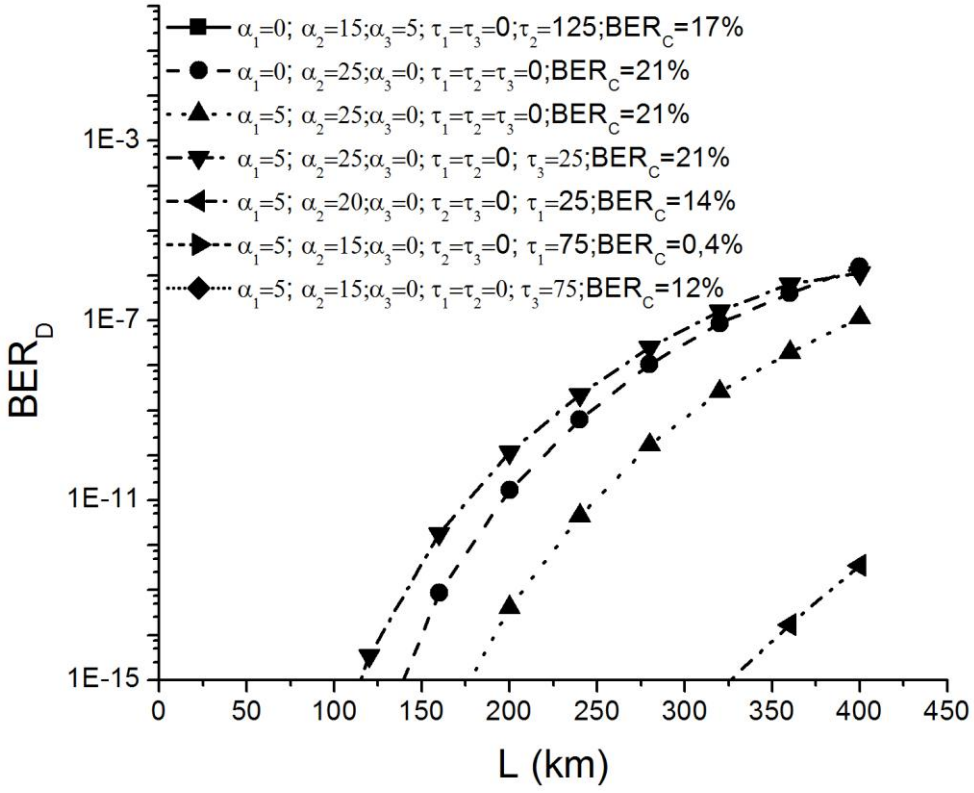

Figura 43 – BER_D em função da distância do enlace de transmissão para diversas combinações chaves criptográficas.

5.3 SIMULAÇÕES NA GRADE DE 50 GHz

Com o objetivo de estudar a adaptabilidade da técnica em transmissões em redes WDM, foi analisado o comportamento da técnica seguindo a regulamentação da ITU-T (ITU-T G.692). Esta análise foi realizada selecionando uma configuração de chave para cada modulação e em sistema *back-to-back* com taxa de 20 Gbits/s.

Para modulação NRZ-OOK utilizou-se a configuração α_1= 0dB, α_2= 30 dB e α_3= 5 dB, com τ_1= τ_2= τ_3= 0 ps. Verificou-se que os resultados apresentados na BER do codificador foi de 47 %. Nota-se que a BER avaliada no codificador está muito próxima à máxima BER possível (50%). Para a BER medida no decodificador, verificou-se que $BER_D < 6x10^{-28}$. Importante notar com isso que tanto a BER no codificador quanto a BER no decodificador são consideradas adequadas quando comparadas às estabelecidas no trabalho.

Para modulação DQPSK utilizou-se a configuração α_1= 0 dB, α_2= 30 dB e α_3= 5 dB, com τ_1= τ_2= τ_3= 0 ps. Verificou-se que os resultados apresentados na BER do codificador foi de 32 %. Para a BER medida no decodificador, verificou-se um valor inferior ao estabelecido no trabalho e muito inferior ao medido para o sinal NRZ-OOK, apresentando um valor de $BER_D < 2x10^{-53}$. Importante notar com isso que tanto a BER no codificador quanto a BER no decodificador são consideradas adequadas quando comparadas às estabelecidas no trabalho.

Esta simulação preliminar demonstrou a aplicabilidade da técnica em canais de 50 GHz. Estudos mais aprofundados ainda devem ser realizados a

fim de verificar o impacto da técnica neste tipo de aplicação. Neste sentido, destaca-se que a técnica não emprega espalhamento espectral no canal, o que pode levar a resultados ainda mais detalhados e positivos para este tipo de aplicação.

6 CONCLUSÕES

Este trabalho apresentou, por meio de simulações computacionais, uma análise do desempenho da técnica de criptografia óptica proposta em (ABBADE, 2012). Em particular, foi avaliada a BER de sinais NRZ-OOK e DQPSK criptografados com perfis de filtros utilizados no mercado. No melhor de nosso conhecimento, esta é a primeira vez que tal análise é realizada. Analisou-se também a influência da mesma técnica sobre a BER na transmissão do sinal codificado por enlaces de até 400 km. Investigou-se também o desempenho da técnica em sistemas de transmissão utilizando a grade de 50 GHz do ITU-T.

É importante notar que a avalição apresentada independe da tecnologia usada para implementar os codificadores e decodificadores ópticos. Em uma primeira abordagem, tal implementação poderia ser feita por meio de elementos discretos, como filtros, atenuadores ópticos e ODLs. Alternativamente, grades de difração, lentes e moduladores espaciais de luz (*spatial light modulators*, SLM) também poderiam ser utilizados em uma configuração próxima àquela indicada em (CORNEJO, 2007). Em uma segunda abordagem, os codificadores e decodificadores também poderiam ser implementados a partir de circuitos integrados de fotônica. Como os elementos que constituem estes dispositivos podem ser passivos, a fotônica de Silício é uma candidata adequada para a implementação de tais circuitos integrados.

Para sinais com modulação NRZ-OOK, a técnica se mostrou eficaz apresentando valores de BER_C entre 17% e 42%, mesmo quando a única componente da chave utilizada era a atenuação. Em todos estes casos, a BER_D apresentou valores inferiores a 10^{-12}. É importante notar que o valor obtido para BER_D só foi adequado após o ajuste do espaçamento entre os filtros, Δf, utilizados para o fatiamento espectral. De fato, sem este ajuste a

BER_D poderia ser tão alta quanto 2%. Desta forma, podemos concluir que com o uso de filtros reais, um valor de Δf maior que a largura de banda do filtro será necessário para garantir BER_D dentro dos valores aceitáveis. Além disso, os valores de Δf podem ser incorporado à chave criptográfica

Adicionalmente, para sinais NRZ-OOK foi estudado o impacto do atraso na técnica. Os resultados demonstraram que quando empregado somente o atraso, a BER_C não superou o mínimo valor considerado (10%). Desta forma, verifica-se que o atraso como chave única não pode ser considerado para um sistema utilizando a chave proposta.

Como análise complementar para sinais NRZ-OOK foram utilizados na mesma chave criptográfica a atenuação e o atraso. Apesar de BER_C apresentar valores adequados (>10%) para qualquer combinação de chave, a BER_D somente apresentou valores adequados ($<10^{-12}$) quando utilizados atrasos inferiores a 50 ps na fatia central. Fato importante foi a necessidade do uso de uma compensação extra de atraso, τ_a, mesmo para níveis de atraso inferiores a 50 ps.

A técnica também se mostrou eficaz para sinais com modulação DQPSK, apresentando valores de BER_C entre 10% e 32% e valores de BER_D inferiores a 10^{-12}. Novamente, observou-se que a aplicação da atenuação de maneira isolada mostrou-se mais eficaz que a utilização isolada de atrasos para aumentar BER_C. É importante ressaltar que para sinais DQPSK a técnica não sofreu restrições quando utilizados atenuação e atraso em conjunto, não sendo necessária uma compensação extra de atraso. Da mesma forma que verificado para o sinal NRZ-OOK, os resultados utilizando a modulação DQPSK foram adequados quando utilizados valores de Δf maiores que a largura de banda do filtro utilizado.

É importante ressaltar o fato que apesar de o atraso não apresentar valores considerados satisfatórios quando utilizado como único componente da chave, o mesmo em conjunto com a atenuação causou um incremento considerável em BER_C. De fato, como mostrado na Figura 34 e na Figura 39 a utilização de atraso pode aumentar a BER do sinal codificado de 10^{-5} para aproximadamente 15%. Conclui-se com isso que o atraso, além de ser mais uma componente da chave, pode gerar um incremento considerável na BER do sinal codificado quando usado em conjunto com a atenuação.

Para analisar a aderência da técnica em sistemas de transmissão ópticos atuais, o sinal codificado foi analisado dentro de um limite de banda de 50 GHz, utilizando para tal um filtro com 20 GHz de largura de banda. Novamente, os resultados apresentaram-se satisfatórios com a utilização de uma taxa de transmissão de bits de 20 Gbps. Para ambas as modulações analisadas, tanto BER_C quanto BER_D apresentaram valores dentro dos limites estipulados neste trabalho.

Destaca-se que o uso de FEC não foi considerado neste trabalho. Em geral, a FEC é utilizada para aumentar o alcance de sistemas ópticos. Sabe-se que com o uso de FEC, uma BER de 10^{-4} pode ser facilmente transformada em uma BER de 10^{-12}, atingindo assim níveis considerados livres de erros. No entanto, quando a criptografia óptica é utilizada, deve-se ter cautela para que a FEC não seja utilizada para possibilitar a decodificação do sinal por receptores não-autorizados. Portanto, quando esta tecnologia for utilizada, haverá um compromisso entre o alcance e a segurança do sistema ópticos.

A partir dos resultados obtidos para sinais NRZ-OOK e DQPSK conclui-se que (i) a técnica é transparente quanto ao uso da modulação; (ii) não causa

espalhamento espectral do sinal; (iii) a princípio não sofre restrições quanto à taxa de transmissão de bits do canal; (iv) possibilita o controle analógico de todas as componentes da chave criptográfica e (v) com o uso de filtros reais deve-se utilizar um espaçamento entre filtros maior que a largura de banda do filtro.

Um futuro trabalho pode ser a analise da técnica aplicada a redes com taxas superiores a 100 Gbps. De fato, sabe-se que para taxas superiores a esta taxa são utilizados equipamentos com dupla polarização por deslocamento de fase diferencial em quadratura (*Dual-Polarization Differential Quadrature Phase Shift Keying*, DP-DQPSK). Este novo trabalho poderia avaliar o uso da técnica em ambas as polarizações do canal DP-DQPSK.

Outra possibilidade é avaliação do grau de robustez da técnica proposta para sinais totalmente ópticos. Esta avaliação poderia levar em consideração o estudo de métodos e processos para assegurar um grau de confiabilidade da técnica em TONs, por meio de práticas e combinações de chaves criptográficas que possam dificultar um receptor não autorizado decodificar o sinal.

Outra abordagem possível é a realização de experimentos que possam comprovar a aplicabilidade da técnica. Isto poderia assegurar a aplicabilidade, como também o grau de confiança que a chave confere ao canal de transmissão (força da chave). Estes experimentos poderiam ser feitos com a utilização de equipamentos discretos (filtros, acopladores, atenuadores e ODLs), ou até mesmo com elementos integrados em fotônica de silício.

TRABALHOS PUBLICADOS

ABBADE, M.L.F.; FOSSALUZZA JR., L.A.; SILVA, R.F.; FAGOTTO, E.A.M. Criptografia Óptica Mediante Controle Analógico da Amplitude e do Atraso de Fatias Espectrais: Análise para Sinais NRZ. MOMAG, 2012. Campinas, Brasil.

APÊNDICE A

A Tabela I apresenta alguns parâmetros importantes relativos aos componentes da simulação utilizados neste trabalho e não mencionados no Capítulo 4. A Tabela II mostra as configurações utilizadas para avaliar a taxa de erro de bit no *software* VPITransmissionMaker.

Tabela I – Parâmetros utilizados no *software* VPITransmissionMaker

ELEMENTO	PARÂMETRO	VALOR/ CONFIGURAÇÃO
Transmissor	Largura de linha	0
Transmissor	Razão de extinção	30
Amplificadores	Figura de ruído	4
Receptor	Responsividade	1
Receptor	Corrente de escuro	0
Receptor	Ruído Térmico	10^{-12}
Receptor	Ruido Shot	Incluso

Tabela II – Parâmetros utilizados para avaliação da BER no *software* VPITransmissionMaker

PARÂMETRO DO *SOFTWARE*	CONFIGURAÇÃO/ VALOR
Tratamento do ruído óptico	Estocástico com análise Gaussiana
BER requerida	10^{-9}
Tipo de amostra	Ótima
Tipo de limite	Ótima
Intervalo de amostras	0

REFERÊNCIAS

ABBADE, M.L.F.; FOSSALUZZA JR., L.A.; SILVA, R.F.; FAGOTTO, E.A.M. Criptografia Óptica Mediante Controle Analógico da Amplitude e do Atraso de Fatias Espectrais: Análise para Sinais NRZ. MOMAG, 2012. Campinas, Brasil.

ABDALLAH, W.; HAMDI, M; BOUDRIGA, N. An All Optical Configurable and Secure OCDMA System Implementation Using Loop Based Optical Delay Lines. IEEE, Icton, 2011.

ABRAMOVICH, F., BAYVEL, P. “Some Statistical Remarks on the Derivation of BER in Amplified Optical Communications Systems,” IEEE Trans. Commun., vol. 45, no. 9, 1997, pp. 1032–1034.

BIRK, M.; GERARD, P.; CURTO, R.; NELSON, L. E.; ZHOU, X. Real-Time Single-Carrier Coherent 100 Gbps PM-QPSK Field Trial. JOURNAL OF LIGHTWAVE TECHNOLOGY, VOL. 29, NO. 4, FEBRUARY 15, 2011.

BREUER, D.; TESSMANN, H.-J.; GLADISCH, A.; FOISEL, H.M.; NEUMANN, G.; REINER, H.; CREMER, H.; , Measurements of PMD in the installed fiber plant of Deutsche Telekom, Holey Fibers and Photonic Crystals/Polarization Mode Dispersion/Photonics Time/Frequency Measurement and Control, 2003 Digest of the LEOS Summer Topical Meetings , vol., no., pp. MB2.1/5- MB2.1/6, 14-16 July 2003

BULOW, H.; BUCHALI, F.; KLEKAMP, A.; , Electronic Dispersion Compensation, Lightwave Technology, Journal of , vol.26, no.1, pp.158-167, Jan.1, 2008

CASTRO, J.; DJORDJEVIC, I.; GERAGHTY, D. Novel Super Structured Bragg Gratings for Optical Encryption. Journal of Lightwave Technology, vol. 24, nº 4, pp. 1875-1885, 2006.

CINCOTTI, G.; SACCHIERI, V.; MAZACCA, G.; KATAOKA, N.; WADA, N.; NAKAGAWA, N. KITAYAMA, K. I. Physical Layer Security: All-Optical Cryptography in Access Networks. IEEE, Icton, 2008.

CORNEJO, J. A.; PEREZ, C. E.; TOCNAYE, J. B. WDM – Compatible Channel Scrambling for Secure High-Data-Rate Optical Transmissions. Journal of Lightwave Technology, vol. 25, pp. 2081-2089, 2007.

ETEMAD, S.; ARGAWAL, A.; BANWELL, T.; JACKEL, J.; MENENDEZ, R.; TOLIVER, P. OCDM-based photonic layer “security” sacalable to 100 Gbits/s for existing WDM network. Journal of Optical Networking, vol. 6, Nº 7, pp.948-967, 2007. New Jersey, USA.

FOSSALUZZA Jr., L. A.; MESSANI, C. A.; TANIGUTI, G. M.; FAGOTTO, E. A. M.; FONSECA, I. E.; ABBADE, M. L. F. All-Optical Cryptography through Spectral Amplitude and Delay Encoding. Trabalho submetido ao Optics Communications.

GERSTEL, O.; JINNO, M.; LORD, A.; BEN YOO. S. J. Elastic Optical Networking: A New Dawn for the Optical Layer?. IEEE Communications Magazine, pp. S12-S20, February 2012.

HARASAWA, K.; HIROTA, O.; YAMASHITA, K.; HONDA, M.; KENICHI, O. SHIGETO, A. TAKESHI, H. YOSHIFUMI, D. Quantum Encryption Communication Over 192-km 2.5-Gbit/s Line With Optical Transceivers Employing. Journal of Lightwave Technology, vol. 29, Nº 3, pp. 316-323, 2011.

HUISZOON, B.; AUGUSTIN, L.M.; HANFOUG, R.; BAKKER, L.; SANDER-JOCHEM, M. J. H.; FLEDDERUS, E. R.; KHOE, G. D.; VAN DER TOL, J. J. G. M.; WAARDT, H.; SMIT, M. K.; KOONEN, A. M. J. Integrated Parallel Spectral OCDMA En/Decoder. IEEE, Photonics Technology Letters, vol.19, no.7, pp. 528-530, 2007.

KAHN, D. The Codebreakers. Macmillan, 2nd Ed., 1.995.

KARTALOPOULOS, S. V. Security in Advanced Optical Communications Networks. IEEE, ICC, 2009. Oklahoma.

KITAYAMA, K. I.; SASAKI, M.; ARAKI, S.; TSUBOKAWA, M.; TOMITA, A.; INOUE, K.; HARASAWA, K.; NAGASAKO, Y.; TAKADA, A. Security in Photonic Networks: Threats and Security Enhancement. Journal of Lightwave Technology, vol. 29, pp. 3210-3222, 2011.

KOSTINSKI, N.; KRAVTSOV, K.; PRUCNAL, P. R. Demonstration of an All-Optical OCDMA Encryption and Decryption System With Variable Two-Code Keying. IEEE Photonics Technology Letters, vol. 20, no. 24, 2008.

LADD, T. D.; JELEZKO, F.; LAFLAMME, R.; NAKAMURA, Y.; MONROE, C.; O'BRIEN, J. L. Quantum computers. Nature, vol. 464, no. 7285, pp. 45-53, 2010.

LATHI, B.P. Modern Digital and Analog Communication Systems. USA: Oxford University Press, 1998.

MARCUSE, D. Derivation of Analytical Expressions for the Bit-Error Probability in Lightwave Systems with Optical Amplifiers, J. Lightwave Technol., vol. 8, no. 12, pp. 1816–1823, 1990.

MUKHERJEE, Biswanath. Optical WDM Networks. Nova Iorque: Springer, 2006.

PONEMOM INSTITUTE LLC. 2011 Cost of Data Breach Study: Global. USA, 2011. Em: < http://www.symantec.com/content/en/us/about/media/pdfs/b-

ponemon-2011-cost-of-data-breach-global.en-us.pdf>. Acesso em: 1 novembro 2012.

PRUCNAL, P. R.; FOK, M. P.; DENG, Y.; WANG, Z. Physical layer security in fiber-optic netwoerks using optical signal processing. SPIE-OSA-IEEE Asia Communications and Photonics. 2009. Vol. 7632, pp. M1-1-M1-10.

RAMASWAMI, R.; SIVARAJAN, K.; SASAKI, G. Optical Networks: A Practical Perspective, Morgan Kaufmann, 3rd edition, 2009.

REIS JR., J.V. Modelagem de Redes CDMA-PON Baseadas em Técnicas de Cancelamento Paralelo e Código Corretores de Erros. Dissertação de Mestrado. São Carlos:Universidade de São Paulo, 2009.

SALEHI, J. A.; BRACKETT, C. A. Code division multiple-access techniques in optical fiber networks-Part II: Systems performance analysis. IEEE Trans. Commun. vol. 37, pp. 834842, Agosto 1989.

SANTOS FILHO, R.V.B. Análise de Sistemas CDMA Ópticos. Dissertação de Mestrado. São Carlos: Universidade de São Paulo, 2006.

SCHWARTZ, M., BENNET, W.R., STEIN, S. Communication Systems and Techniques. New York: McGraw-Hill, 1966, Appendix B.

SHANEMAN, K. & GRAY, S. Optical Network Sevcurity: Technical Analysis of Fiber Tapping Mechanisms and Methods for Detection & Prevention. Milcon, 2004. IEEE Military Communication Conference, 2004 p. 711-717, New York.

SUCHAT, S.; PAIBOOD, S.; YUPAPIN, P. P. An Experiment of Optical Encryption Technique with Quantum Security for Mobile Phone Up-link Converter. IEEE ICIT, 2002. Bangkok,Thailand.

TAJAHUERCE, E.; MATOBA, O.; VERRAL, S.C.; JAVIDI, B. Optoeletronic information encryption with phase-shifting interferometry. Applied Optics, Optical Society of America, 2000, Vol. 39, nº 14, pp.2313-2320.

TANAKA, A.; FUJIWARA, M.; NAM, S. W.; NAMBU, Y.; TAKAHASHI, S.; MAEDA, W.; YOSHINO, K.; MIKI, S.; BAEK, B.; WANG, Z.; TAJIMA, A.; SASAKI M.; TOMITA, A. Ultrafast quantum key distribution over a 97 km installed telecom fiber with wavelength division multiplexing clock synchronization. Optical Express, 2008. Vol. 16, pp. 11354-11360.

TANENBAUM, ANDREW N. Computer Network. Prentice Hall; 4 edition. August 19, 2002.

TOCNAYE, J.L.B.; CORNEJO, J.A. Implementation of a Noninvasive Data Encryption Technique Based on a Free-Space Spectral Phase Scrambling Scheme. Optical Engineering, vol. 47, nº 6, pp. 65004-1-65004-9, 2008.

TOWNSEND, P. Quantum Cryptografhy in Optical Fiber Networks. BT Laboratories, United Kingdom, 1998.

VPIPHOTONICS. Receiver with Deterministic and Stochastic BER Estimation. Somerset: VPITransmissionMaker, 2011, Rx_OOK_BER.

WANG, X.; WADA N. Spectral phase encoding of ultra-short optical pulse in time domain for OCDMA application. Optics Express, vol. 15, pp. 7319-7326, 2007.

WANG, X.; WADA, N.; HAMANAKA, T.; MIYAZAKI, T.; CINCOTTI, G.; KITAYAMA, K. I. OCDMA over WDM Transmission. Transparent Optical Networks, pp. 110 -113, 2007.

YIN, H.; RICHARDSON, D. J. Optical Code Division Multiple Access Communication Networks – Theory and Applications. Tsinghua University Press and Springer-Verlag, 2007. 382 p.

YUEN, H.P. Security and efficiency of quantum cryptographic protocols. LEOS Summer Topical Meetings, pp. 30 - 31 , 2006