

PONTIFÍCIA UNIVERSIDADE CATÓLICA DE CAMPINAS
CENTRO DE CIÊNCIAS EXATAS, AMBIENTAIS E DE TECNOLOGIAS

CARLOS ALBERTO MESSANI

CRIPTOGRAFIA ÓPTICA BASEADA EM FATIAMENTO ESPECTRAL

CAMPINAS
2014

PONTIFÍCIA UNIVERSIDADE CATÓLICA DE CAMPINAS
CENTRO DE CIÊNCIAS EXATAS, AMBIENTAIS E DE TECNOLOGIAS

CARLOS ALBERTO MESSANI

CRIPTOGRAFIA ÓPTICA BASEADA EM FATIAMENTO ESPECTRAL

Dissertação apresentada como exigência para
obtenção do Título de Mestre em Engenharia
Elétrica, ao Programa de Pós-Graduação Stricto
Sensu em Engenharia Elétrica, Pontifícia
Universidade Católica de Campinas.

Orientador: Prof. Dr. Marcelo Luís Francisco Abbade

CAMPINAS

2014

CARLOS ALBERTO MESSANI

**CRIPTOGRAFIA ÓPTICA BASEADA EM FATIAMENTO
ESPECTRAL**

Dissertação apresentada ao Programa de Pós-Graduação em Engenharia Elétrica 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 Luis Francisco Abbade

Dissertação defendida e aprovada em 27 de junho de 2014 pela Comissão Examinadora constituída dos seguintes professores:

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

Prof. Dr. Eric Alberto De Mello Fagotto
Pontifícia Universidade Católica de Campinas



Prof. Dr. Lucas Heitzmann Gabrielli
Universidade Estadual de Campinas

Ficha Catalográfica

Elaborada pelo Sistema de Bibliotecas e

Informação – SBI – PUC-Campinas

t005.82 Messani, Carlos Alberto.
M583c Criptografia óptica baseada em fatiamento espectral / Carlos Alberto
Messani. - Campinas: PUC-Campinas, 2014.
94p.

Orientador: Marcelo Luís Francisco Abbade.
Dissertação (mestrado) – Pontifícia Universidade Católica de
Cam-pinas, Centro de Ciências Exatas, Ambientais e de Tecnologias,
Pós-Graduação em Engenharia Elétrica.
Inclui bibliografia.

1. Criptografia de dados (Computação). 2. Fibras óticas. 3. Telecomunicações. 4. Redes de computadores. I. Abbade, Marcelo Luís Francisco. II. Pontifícia Universidade Católica de Campinas. Centro de Ciências Exatas, Ambientais e de Tecnologias. Pós-Graduação em Engenharia Elétrica. III. Título.

22.ed. CDD – t005.82

Dedico este trabalho aos meus pais, Pedro Messani e Lída Messani,
ao meu filho Fábio Messani,
e às minhas irmãs Ana, Vumi, Mpava e Suzana

AGRADECIMENTOS

Antes de tudo e qualquer coisa, agradeço muito a Deus. Nessa longa trajetória muitas provas ele me tem dado de que está comigo e tem acompanhado todos os meus passos. Resumidamente, vou agradecer os meus pais, Pedro Baptista Messani e Lídia dos Santos Araújo Messani. Agradeço de forma resumida, pois se for mencionar a imensidão do que eles fizeram e continuam a fazer por mim, acho que daria outra dissertação... O apoio moral e material de maneira inquestionável vindo dos meus pais não há preço que pague.

Às minhas irmãs, Ana Messani, Vumi Messani, Mpava Messani e a minha irmãzinha mais nova, Suzana Messani, deixo registrado aqui o meu muito obrigado por tudo, pois se tudo deu certo é porque elas sempre estiveram comigo e dando o maior apoio. Agradeço também o meu filho, Fábio Messani, pois direta ou indiretamente, ele foi a minha fonte de energia para continuar. Jamais me esqueceria de agradecer a Camila Uemura, porque todas as palavras ainda seriam poucas para expressar o quão ela foi e continua sendo importante na minha trajetória.

Agradeço também o Prof. Dr. Marcelo Abbade, que fez por mim muito mais do que a sua obrigação, foi muito mais do que um simples Professor/Orientador. Indiretamente, tive um coordenador, o Prof. Dr. Eric Fagotto, no qual sou muito grato por inúmeras contribuições no meu trabalho e intelectualmente.

Não menos importante, agradeço os meus colegas e companheiros do grupo de pesquisa, Cleiton de Jesus Alves e Guilherme Minoru Taniguti, Gabriel Suzigan, que foram os meus grandes suportes desde o primeiro dia de curso.

À Pontifícia Universidade Católica de Campinas, por ter propiciado a estrutura necessária e pela bolsa de estudo parcial.

À FAPESP e ao CNPq pelo financiamento parcial deste trabalho, dentro do escopo do Programa FOTONICOM.

À VPIphotonics™ por fornecer licenças acadêmicas do software de simulação utilizado neste trabalho.

FRASE

*A mente que se abre a uma nova ideia
jamais voltará ao seu tamanho original.*

Albert Einstein

RESUMO

As redes ópticas têm evoluído significativamente nos últimos anos. Apesar dessa evolução, a camada física dessas redes ainda apresenta vulnerabilidades para diversos tipos ataques, incluindo espionagem, interceptação, bloqueio e ataques à infraestrutura física. Para combater ou prevenir as redes desses ataques, é essencial que se adote técnicas que garantam o sigilo das informações. Neste contexto, este trabalho apresenta uma nova técnica de criptografia óptica baseada em fatiamento espectral. Nesta técnica, a codificação é realizada por meio da divisão do sinal óptico em n fatias espectrais. Após a divisão, o sinal de cada fatia passa por um filtro óptico passa banda que tem a função de alocar cada fatia espectral numa determinada frequência. Posteriormente, o sinal pode ser submetido a dois estágios de codificação. No primeiro estágio é realizada a codificação de fase espectral. Nesta a codificação é feita por desvio de fase. No segundo, a codificação é feita por meio de atraso dos bits/símbolos, esta é denominada codificação espectral por atraso. A recuperação do sinal é realizada no decodificador por intermédio da compensação das fases e Atrasos inseridos em cada fatia espectral do codificador. As medições da relação sinal-ruído óptico e das taxas de erro de bits dos sinais codificados, BER_C , e decodificados, BER_D , foram adotadas como critérios de avaliação da robustez técnica. O desempenho da técnica foi investigado por intermédio de simulação com o software *VPI Transmission Maker versão 9.0*. Nestas simulações, foram avaliados os sinais nos domínios do tempo e frequência. Foram realizadas simulações com os sinais modulados por

chaveamento diferencial de fase (*Differential Phase Shift Keying, DPSK*), deslocamento de fase *diferencial em quadratura (Differential Quadrature Phase Shift Keying, DQPSK)* e modulação de amplitude em quadratura de 16 símbolos (*Quadrature amplitude modulation, 16-QAM*), com as taxas de transmissões de 40 Gbps para os sinais *DPSK* e *DQPSK* e 200 Gbps para os sinais 16-QAM. Os resultados das simulações foram satisfatórios, em todos os casos, BER_C foram superiores a 10% de degradação dos sinais e no decodificador BER_D foram inferiores a 10^{-15} que é considerada livre de erros de bits.

ABSTRACT

Optical networks have been evolving significantly over the years. Despite this evolution, the physical layer of these networks still have vulnerabilities to several kinds of attacks including eavesdropping, interception, jamming, and attacks on physical infrastructure. To combat or prevent these networks attacks, the adaption of techniques to ensure the confidentiality of information is essential. In this context, this presents a new technique of optical encryption based on spectral slicing. In this technique, coding is performed by dividing the optical signal into n spectral slices. After the signal is split, each slice passes through an optical bandpass filter that has function of allocate each spectral slice to a particular frequency. Subsequently, the signal will be submitted to another two stages of encoding, as following. At first stage the signal will receive a phase shift, we call this stage as Phase-Shift Encoding. After that in the following stage it will receive a signal delay in bits per symbol, this is called the delay spectral coding. The signal deciphering is performed at the decoder stage, by removing phases and delays inserted in each spectral slice during the encoding process. Measurements of the optical signal to noise ratio and bit error rate of coded signals, BER_C , and decoded, signals BER_D , were used as parameter to evaluate the robustness of the technique. The technique performance was evaluated by simulation on software VPI Photonics[®], on Transmission Maker version 9.0. In these simulations, we studied the signals in time and frequency domains, using several modulation techniques like Differential Phase Shift Keying (*DPSK*), Differential Quadrature Phase Shift Keying (*DQPSK*), 16 symbols quadrature amplitude modulation (16 - QAM), with rates of 40 Gbps for *DPSK* and

DQPSK signals and 200 Gbps for 16-QAM signals. The simulation results were satisfactory in all cases: BER_C exceeds 10% degradation of the signals and the decoder BERD was less than 10⁻¹⁵, which is considered an error free transmission.

LISTA DE FIGURAS

Figura 1 – <i>Porcentual de assinaturas em banda larga fixa por regiões até o final de 2014, em milhões</i>	1
Figura 2 - Porcentual de acessos à internet por indivíduo até o final de 2014	2
Figura 3 - Crescimento do consumo do tráfego	3
Figura 4 – Técnica de criptografia usada em	6
Figura 5 – Técnica de criptografia adotada	6
Figura 6 - Disposição dos filtros no domínio da frequência.....	14
Figura 7 - Diagrama de bloco da técnica de codificação do sinal óptico	15
Figura 8 - Diagrama de bloco do decodificador óptico	16
Figura 9 - Ciclo trigonométrico para a relação entre fase	18
Figura 10 - Diagrama de bloco usado para simulações back-to-back.....	19
Figura 11 – Representação dos perfis dos filtros utilizados	22
Figura 12 - representações das sequências de bits dos sinais, (a) gerado pelo transmissor, (b) codificado e (c) decodificado	25
Figura 13 - Espectros óptico dos sinais, (a) transmitido, (b) codificado e (c) Decodificado	29
Figura 14 - Influência do atraso em BER _c em função das fatias espectrais	30
Figura 15 - Influência da fase na BER _c em função da fatia espectral.....	32
Figura 16 - Gráfico Influência do número e posição das fatias espectrais em BER em função da OSNR	34

Figura 17 - Representações das sequências de bits dos sinais, (a) gerado pelo transmissor, (b) codificado e (c) decodificado.....	36
Figura 18 - Diagramas de olho dos sinais, (a) gerado pelo transmissor, (b) codificado e (c) decodificado.....	39
Figura 19 - Espectros ópticos dos sinais DQPSK transmitido, (b) Sinal codificado, (c) Sinal decodificado.....	40
Figura 20 - Influência do atraso em BER_c em função da fatia espectral.....	41
Figura 21 - Influência da fase na BER_c em função da fatia espectral.....	43
Figura 22 - Influência do número e posição das fatias espectrais na BER em função da OSNR.....	44
Figura 23 - Diagramas de constelações referentes aos sinais, (a) gerado pelo transmissor, (b) codificado e (c) decodificado.....	47
Figura 24 - Espectros ópticos dos sinais, (a) gerado pelo transmissor, (b) codificado e (c) decodificado.....	49
Figura 25 - Influência do atraso na taxa de erro de bits do sinal codificado em função da fatia espectral.....	50
Figura 26 - Influência de φ_C em BER_c em função da fatia espectral.....	52
Figura 27 - Influência do número e posição das fatias espectrais na BER_c	53
Figura 28 - Disposição dos filtros em frequência. (a) Filtros ideais com perfis retangulares, (b) Filtros reais super gaussianos de 5 ordem.....	56
Figura 29 -Fatiamento espectral do sinal 16-QAM mediante a utilização de filtragem digital de Nyquist.....	57
Figura 30 - Resultados de simulações com sinais 16-QAM em 350 km.....	58

Figura 31 – Esquemático das simulações com 14 fatias	59
Figura 32 - Resultados de simulação com 14 fatias para sinais 16-QAM em 350 km.	60
Figura 33 – Esquemático das simulações com duas codificações.....	61
Figura 34 - Resultados de simulação com 2 codificações para sinais 16-QAM em 350 km (a) Sinal no codificador 1, (b) Sinal no codificador 2, (c) Sinal no decodificador 2	62
Figura 35 – Influência do número e posição da fatia.....	63

LISTA DE TABELAS

Tabela 1 - Parâmetros utilizados nas simulações	20
Tabela 2 - Resultada de simulações da COBFE com 14 fatias.....	60
Tabela 3 - Resultado de simulações da COBFE com duas codificações.....	62

LISTA DE SIGLAS E ABREVIATURAS

a.C	Antes de Cristo
AON	<i>All-Optical Network</i>
BER	Taxa de Erro de Bits
COBFE	Criptografia Óptica Baseada em Fatiamento Espectral
DPSK	<i>Differential Phase Shift Keying</i>
DQPSK	<i>Quadrature phase-shift keying</i>
DSL	<i>Digital Subscriber Line</i>
EAD	Educação à Distância
FEC	<i>Forward Error Correction</i>
HDTV	<i>High-Definition Television</i>
ITU	<i>International Telecommunication Union</i>
OBPF	<i>Optical Band Pass Filter</i>
OCDMA	<i>Optical Code Division Multiple Access</i>
OSI	<i>Open Systems Interconnection</i>
OSNR	<i>Optical Signal-to-Noise Ratio</i>
PRBS	<i>Pseudo Random Binary Sequence</i>
QoS	<i>Quality of service</i>
SAE	<i>Spectral Amplitude Encoding</i>
SBS	<i>Stimulated Brillouin Scattering</i>

SDE	<i>Spectral Delay Encoding</i>
SPE	<i>Spectral Phase Encoding</i>
TELEBRASIL	Associação Brasileira de Telecomunicações
TON	<i>Transparent Optical Networks</i>
EDFA	Amplificador óptico à fibra dopada com érbio do codificador
16-QAM	<i>Quadrature amplitude modulation 16 symbols</i>
WDM	<i>Wavelength-division multiplexing</i>

LISTA DE SÍMBOLOS

τ	Atraso
α	Atenuação
φ	Fase
τ_{Ci}	Atraso do codificado
φ_{Ci}	Fase do codificador
τ_{Di}	Atraso do decodificado
θ_i	Ângulo de incremento para completar 360 graus
$\tau_{máxi}$	Atraso máximo
$\alpha_{máx}$	Atenuação máxima
$EDFA_D$	Amplificador óptico à fibra dopada com érbio do decodificador
$EDFA_E$	Amplificador óptico à fibra dopada com érbio do codificador

Sumário

1.	INTRODUÇÃO.....	1
1.1.	Conceitos de criptografia	5
1.2.	Revisão da literatura	7
1.3.	Contribuições do trabalho	11
1.4.	Organização do trabalho.....	11
2.	CRIPTOGRAFIA ÓPTICA BASEADA EM FATIAMENTO ESPECTRAL – <i>COBFE</i>	13
2.1.	Princípio da <i>COBFE</i>	13
2.2.	Arranjos das simulações <i>back-to-back</i>	19
2.3.	Comparações entre a <i>COBFE</i> e trabalhos relacionados	21
2.4.	Perfis dos <i>OBPF</i> utilizados	22
3.	ANÁLISE DOS RESULTADOS DAS SIMULAÇÕES DA <i>COBFE</i> PARA SINAIS DPSK.....	24
3.1.	Análise dos resultados nos domínios do tempo e da frequência	25
3.1.1.	Sequências temporais	25
3.1.2.	Diagramas de olho.....	27
3.1.3.	Espectros ópticos	28
3.2.	Influência do atraso na taxa de erro de bits do sinal codificado em função da fatia espectral	29

3.3. Influência da fase na taxa de erro de bits do sinal codificado em função da fatia espectral	31
3.4. Influência do número e posição das fatias espectrais na taxa de erro de bits do sinal decodificado em função da relação sinal-ruído óptica.....	33
4. ANÁLISE DOS RESULTADOS DAS SIMULAÇÕES DA COBFE PARA SINAIS <i>DQPSK</i>	35
4.1. Análise dos resultados nos domínios do tempo e da frequência	36
4.1.1. Sequências temporais	36
4.1.2. Diagramas de olho.....	38
4.1.3. Espectros ópticos	40
4.2. Influência do atraso na taxa de erro de bits do sinal codificado em função da fatia espectral	41
4.3. Influência da fase na taxa de erro de bits do sinal codificado em função da fatia espectral	42
4.4. Influência do número e posição das fatias espectrais na taxa de erro de bits do sinal decodificado em função da relação sinal-ruído óptica.....	44
5. ANÁLISE DOS RESULTADOS DAS SIMULAÇÕES DA COBFE PARA SINAIS 16-QAM.....	46
5.1 Diagramas de constelações.....	47
5.2 Análise dos espectros ópticos.....	48

5.3	Influência do atraso na taxa de erro de bits do sinal codificado em função da fatia espectral	50
5.4	Influência da fase na taxa de erro de bits do sinal codificado em função da fatia espectral	51
5.5	Influência do número e posição das fatias espectrais na taxa de erro de bits do sinal codificado em função da relação sinal-ruído óptica.....	53
6.	ANÁLISE DOS RESULTADOS DE SIMULAÇÕES MEDIANTE A UTILIZAÇÃO DE FILTRAGEM DIGITAL DE NYQUIST E FILTROS ÓPTICOS SUPERGAUSSIANOS DE 5 ORDEM.....	55
6.1.	Fatiamento Espectral	56
6.2.	Resultados de simulações de propagação em rede.....	57
6.3.	Resultados de simulação de propagação em rede com sinal codificado com em 14 fatias	58
6.4.	Resultados de simulação com duas codificações	60
6.5.	Influência do número e posição das fatias espectrais na taxa de erro de bits do sinal decodificado em função da relação sinal-ruído óptica	63
7.	CONCLUSÃO.....	64
8.	REFERÊNCIAS	70

1. INTRODUÇÃO

Segundo levantamento da União Internacional das Telecomunicações (UIT) [1], estima-se que até o final de 2014 a penetração da banda larga fixa no mundo registre um crescimento de cerca de 10%. Sendo deste crescimento, 44% de assinaturas serão registradas na Ásia e Pacífico, e 25% na Europa. Nas regiões das Américas, estima-se que a taxa de penetração atinja apenas 2,5% até ao final de 2014. Em contraste, apesar de o continente africano ter registrado um crescimento de dois dígitos em um período de quatro anos, este corresponde apenas a 0,5% da taxa mundial. A Fig. 1 ilustra o percentual de assinaturas em banda larga fixa por regiões até 2014.

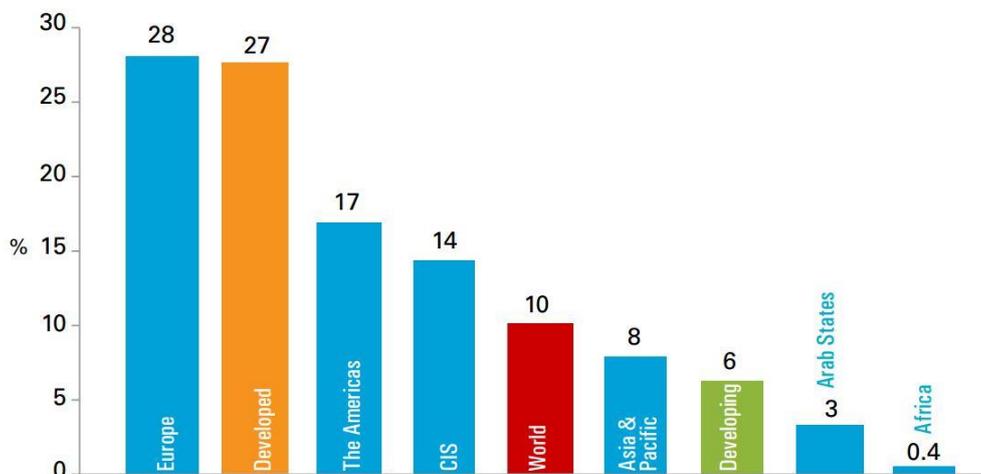


Figura 1 – Porcentual de assinaturas em banda larga fixa por regiões até o final de 2014, em milhões.

Fonte: União Internacional das Telecomunicações

Apesar de a taxa de crescimento da penetração da banda larga fixa no continente americano ser relativamente baixa (2,5%), segundo levantamento da

Associação Brasileira de Telecomunicações (Telebrasil), no primeiro trimestre de 2014, o número de acessos em banda larga no Brasil foi de aproximadamente 145,6 milhões, que corresponde a um crescimento de 51% com relação ao mesmo período do ano anterior [2, 3].

Ainda segundo [1], em 2010, a população africana com acesso à internet era estimada em apenas 10%. Para o final de 2014, estima-se que este número atinja os 20%. No continente americano, a estimativa é que o número de usuários de internet chegue perto de duas a cada três pessoas. Na Europa, a expectativa é que o acesso à Internet atinja 75% da população até o final de 2014, tal como ilustra a Fig. 2. Até o momento, este é o maior índice registrado, visto que, a estimativa para o continente asiático é de 45%.

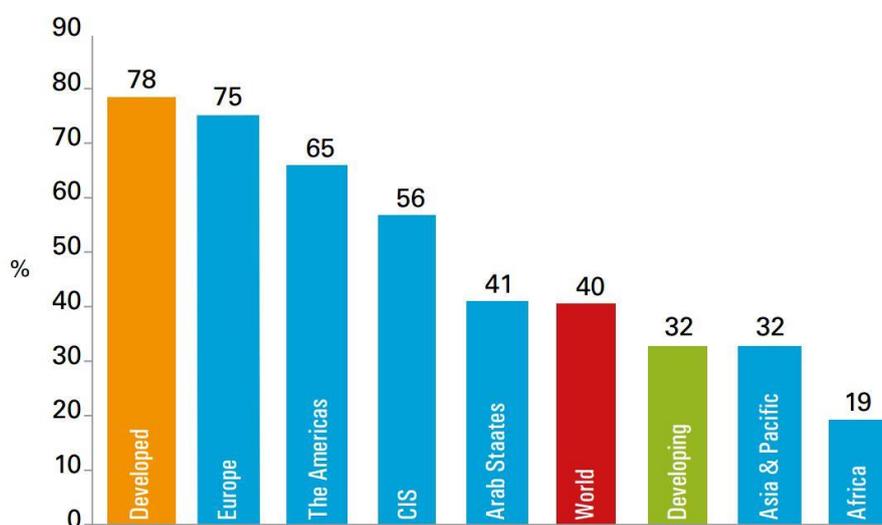


Figura 2 - Porcentual de acessos à internet por indivíduo até o final de 2014

Fonte: União Internacional das Telecomunicações

Além do crescimento exponencial do número de acessos à banda larga, o aumento de banda larga consumida deve-se também a aplicações e tipos de

serviços que cada vez mais vêm necessitando de maior largura de banda para suportar aplicações emergentes, tais como vídeo sob demanda (*video on demand, VoD*), televisão de alta definição (*high-definition television, HDTV*), educação à distância (*EAD*), sistemas médicos de alta resolução, transmissões de áudio com alta qualidade que requerem uma alta largura de banda tanto no *downstream* quanto no *upstream*, etc [3-6].

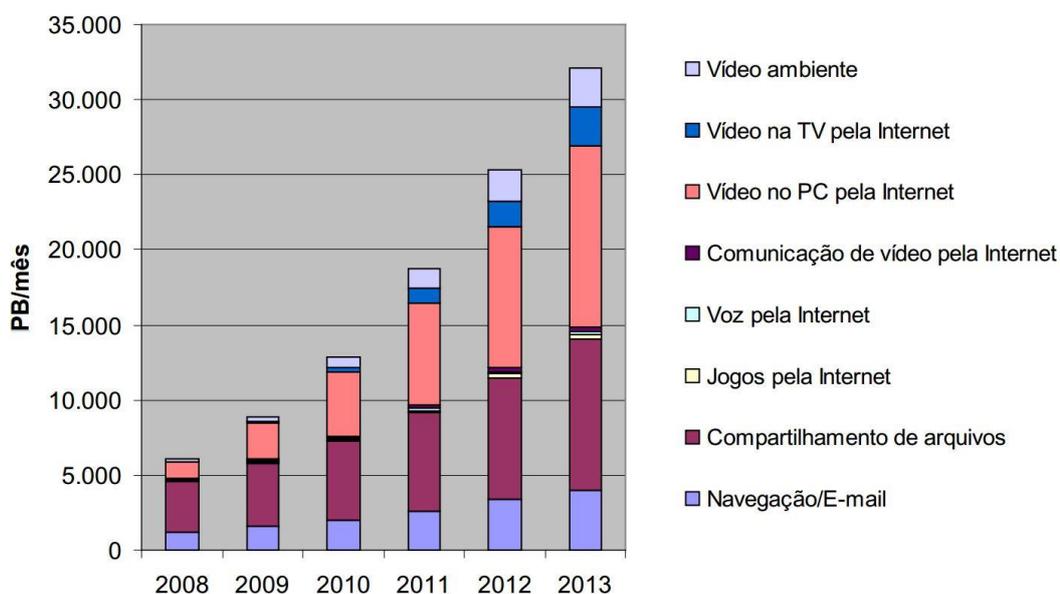


Figura 3 - Crescimento do consumo do tráfego

Vale salientar que, segundo [7], para que a atual necessidade de largura de banda seja relativamente suprida, seriam necessários, no mínimo, 100 *Mbps* bidirecionais para cada usuário. Muito embora o número de usuários com acesso à Internet com altas taxas de transmissão seja ainda relativamente baixo, dados mostrados anteriormente indicam que o tráfego nas redes de acesso vem crescendo de maneira exponencial. Neste contexto, vem elevando-se também o número de empresas de diferentes setores que aderem a esses serviços. Geralmente, empresas que efetuam transações bancárias, militares e algumas governamentais têm um grau de exigência maior no quesito segurança nas

transmissões. Deste modo, é essencial que se adote técnicas que garantam sigilo das informações na rede [8, 9].

A segurança em redes consiste em garantir a integridade dos dados, estar livre de acesso não autorizado de recursos computacional e livre de espionagem ou escutas telefônicas. De maneira geral, consiste em estar livre de interrupção de serviços [10]. Assim, tal como nenhuma propriedade física é absolutamente segura, nenhuma rede também é totalmente segura contra ataques.

Do ponto de vista das infraestruturas de rede, as redes ópticas totalmente ópticas (*All-OPTICAL Networks, AONs*) são mais seguras do que as demais redes de comunicação. Ainda assim, as *AONs* apresentam algumas vulnerabilidades a alguns equipamentos, como por exemplo, acopladores ópticos passivos *clip-on* (modelo *Altesys PFC1000*) que podem ser encontrados no mercado por preços relativamente baixos [11, 12].

As contramedidas de segurança aplicadas nas redes de comunicação tradicionais podem ser aplicadas também nas *AONs*. Entre essas, destacam-se a prevenção, detecção e reação. A Prevenção implica em fortalecimento dos componentes da rede com técnicas de proteção, como por exemplo, criptografia de dados [10]. A Detecção consiste em identificar possíveis ameaças, ou seja, localizar a origem do ataque. Por outro lado, a reação significa isolar ou contra atacar, ou também, reconfiguração da rede.

Nas *AONs* a contramedida mais importante para garantir a segurança é a prevenção, que consiste em aplicar técnicas de criptografia dos dados. Muito embora a criptografia seja mais aplicada na camada de apresentação do modelo

de Interconexão de Sistemas Abertos (*Open Systems Interconnection, OSI*), estudos sugerem que quanto maior for o número de camadas em que a criptografia for aplicada, maior é a segurança dos dados [13]. Por não se tratar do foco deste trabalho, as contramedidas de detecção e reação não serão abordadas com mais detalhes. Porém, os leitores interessados poderão consultar em [13].

O restante deste capítulo está organizado da seguinte maneira. Na Seção 1.1 serão abordados aspectos históricos sobre a criptografia. Posteriormente, na Seção 1.2 serão apresentados alguns trabalhos sobre criptografia óptica disponíveis na literatura. As contribuições deste trabalho serão mencionadas na Seção 1.3. Finalizando o capítulo, a Seção 1.4 descreverá a organização desta dissertação.

1.1. Conceitos de criptografia

De maneira geral, a criptografia é comumente definida como a arte de escrever em códigos ou cifras, de modo que só quem conhece as características da codificação possa ler a referida mensagem. Estudos revelam que essa estratégia de codificar mensagens é quase tão antiga quanto a escrita em si [14]. Segundo indícios, na Antiguidade, a criptografia já era conhecida na China, Egito, Mesopotâmia e Índia, mas sua exata origem é ainda desconhecida.

Em Esparta, 400 a.C., uma das técnicas utilizadas para codificar mensagens envolvia uma tira de pergaminho de forma espiral ao longo de um bastão cilíndrico. Longitudinalmente, o texto era escrito de modo que cada letra ficasse separada numa das voltas do papiro [14]. Quando desenrolada a faixa,

viam-se as letras dispostas sem qualquer sentido. Para ler a mensagem, seria necessário enrolar em um bastão com o mesmo diâmetro daquele em que foi escrita a mensagem, como mostrado na Fig. 4.



Figura 4 – Técnica de criptografia usada em Esparta 400 anos antes de Cristo

Na Roma antiga, Júlio César havia adotado um método para codificar suas mensagens. Neste método cada letra do texto era substituída pela terceira letra do alfabeto contando a partir da sua posição [14], tal como pode ser observado na Fig.5. De fato, esse método apresenta um nível baixo de segurança.

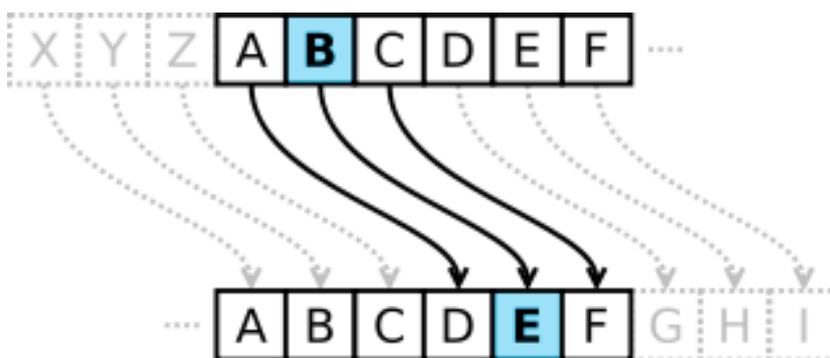


Figura 5 – Técnica de criptografia adotada por Júlio César na Roma Antiga

Desde os primeiros registros da utilização de técnicas de criptografia, ou seja, técnicas artesanais, até a presente data, a criptografia vem registrando

valiosos avanços no que diz respeito à robustez. Isso se deve à crescente evolução das tecnologias e supercomputadores que vêm potencializando a capacidade de realizar cálculos cada vez mais complexos e criptografar mensagens relativamente grandes em curto período [14]. De fato, os métodos para anular essas criptografias também têm acompanhado tal evolução.

Em tempos modernos existem vários métodos de efetuar a criptografia. Geralmente esses métodos são baseados em chaves simétricas e assimétricas [15, 16]. Os métodos de criptografia que utilizam chaves simétricas e assimétricas são utilizados para codificar dados. A seção seguinte abordará algumas das técnicas de criptografia na camada física/óptica apresentadas na literatura.

1.2. Revisão da literatura

Uma das maneiras de realizar criptografia no domínio óptico é por meio da técnica chamada criptografia caótica. Um estudo apresentado em [17] avalia a utilização de sinais caóticos para codificação de informações em transmissões de redes ópticas. Neste método, a onda óptica da portadora gerada por um laser caótico é usada para codificar os dados. Segundo os autores, foram realizados experimentos para transmissões de até 120 *km*. A decodificação do sinal é realizada por intermédio de um segundo laser que sincroniza com o transmissor caótico. Para os autores, o sistema de codificação baseado em sinais caóticos é aplicável em redes *WDM*, desde que a largura da portadora caótica seja menor que o espaçamento entre os canais *WDM*.

Em [18], foi apresentado um estudo para avaliar a vulnerabilidade da criptografia caótica contra a filtragem não-linear. Nesse mesmo estudo, foi aplicado um método de filtragem com base na equação de *Ginzburg Landau*. Segundo [18], este método é capaz de detectar mudanças em uma série de dados, com alguns ajustes, é possível quebrar os esquemas de codificação nos casos em que a alteração na potência média pouco induzida pela codificação de dados é maior do que a induzida pelas flutuações caóticas. O autor defende também que, a filtragem não-linear, para o efeito, é superior aos filtros lineares, isso deve-se ao fato de que além de efetuar a filtragem dos sinais caóticos com mais rapidez do que o filtro não-linear, a não-linearidade aumenta o contraste dos bits 1 e 0. Assim, melhoraria a qualidade e os dados poderiam ser recuperados. Ainda segundo [18], se a criptografia caótica for realizada sem preservar a potência média dos bits 1 e 0, a amplitude de codificação deve ser da mesma ordem ou menor do que as variações do valor do sinal caótico. Caso contrário, um intruso teria alguma facilidade em invadir a rede.

Outra estratégia interessante para criptografar opticamente sinais é a criptografia quântica. Um estudo sobre a criptografia quântica em redes ópticas foi realizado por Paul D. Townsend [19]. Neste trabalho, foram abordados sistemas interferométricos que operam no comprimento de onda de $1,3 \mu m$ por meio de um enlace ponto-a-ponto de até $50 km$ com multiusuários passivos na rede. O autor descreve também o comportamento da rede usada e são discutidas questões relacionadas com a interferência entre canais de dados convencionais propagados em diferentes comprimentos de onda.

Stamatios V. Kartalopoulos *et al.* [20], realizaram estudos para avaliar a vulnerabilidade da criptografia quântica em transmissão de dados. Concluíram

que a criptografia quântica, no atual estado, não fornece uma tecnologia robusta quanto o esperado. Neste mesmo estudo, o autor defende que as fontes de fótons dos dispositivos lasers em estado sólido não geram os fótons de maneira individual, mas sim, uma multiplicidade fótons. Além destes, o estado de polarização dos fótons provenientes de lasers não pode ser controlado com facilidade. Outra conclusão está relacionada com a aplicação da criptografia quântica em topologias de redes totalmente ópticas e opticamente transparentes. Nestas redes não há garantias de que a polarização dos fótons não seja alterada. Conseqüentemente, o desempenho da criptografia quântica fim-a-fim em algumas dessas redes é questionado. Segundo o autor, este questionamento deve-se ao fato de que há uma birrefringência residual que é medida como a diferença de índices de refração na direção x e y da fibra (z é o sentido de transmissão). Além disso, o autor também defende que a fibra óptica para criptografia quântica deve ser contínua, sem emendas e sem conectores, visto que, estes podem alterar o estado de polarização dos fótons transmitidos de uma extremidade da fibra para outra. Com comprimentos de fibra muito longos seria necessária a utilização de amplificadores ópticos por volta de 60 a 100 *km*. No entanto, a utilização de amplificadores ópticos no enlace não manteria o estado de polarização e a utilização de repetidores tornaria a rede mais vulnerável a espionagens.

Cornejo *et al* [21], apresentam uma técnica de criptografia óptica baseada na codificação espectral por diferenciação de fase utilizando uma máscara de difração dispersiva de *Bragg*. Nesta técnica o sinal óptico que incide sobre a grade de difração é separado em diversas componentes espectrais. Em seguida,

o sinal é submetido a uma máscara de difração dispersiva de *Bragg* composta de vários pixels que tem a função de filtrar parte de componentes do sinal. A fase de cada componente é variada por intermédio de uma tensão aplicada a cada pixel. A variação de cada componente espectral causa um alargamento temporal que distorce o sinal tornando-o ilegível. Neste estudo, o autor avalia a *OSNR* e são considerados aspectos relacionados à dispersão e que pudessem interferir na qualidade ou distância de propagação.

Além dos trabalhos sobre criptografia óptica apresentados nessa seção, outras abordagens podem ser encontradas no Capítulo 7 [22-27]. Vale salientar que abordagens sobre a criptografia óptica não se resumem apenas aos trabalhos mencionados aqui, outros trabalhos podem ser encontrados na literatura.

Neste trabalho é avaliada a técnica de criptografia totalmente óptica baseada no fatiamento espectral (*COBFE*), inicialmente proposta na literatura em [28]. Essa técnica efetua a criptografia por intermédio da degradação artificial do sinal. Para isso, o espectro do sinal óptico é dividido em diversas fatias espectrais e cada uma dessas fatias é submetida a uma dada degradação que torna o sinal ilegível. Para recuperar o sinal degradado, o decodificador precisa conhecer os parâmetros usados para codificar. Algumas comparações entre a *COBFE* e trabalhos apresentados na literatura serão abordadas na Seção 2.3.

1.3. Contribuições do trabalho

Este trabalho continua os estudos da *COBFE* inicialmente apresentado em [28]. Em particular, são apresentadas três contribuições principais. A primeira é que, diferente de outros trabalhos que avaliam a codificação em atraso e amplitude [28-31], neste trabalho considera-se a codificação em atraso e fase. Nota-se que em [28-31], a codificação em amplitude marca o espectro, o que facilitaria a identificação da chave por um invasor ou alguém não autorizado. De fato, tal comportamento não é observado na codificação em fase. A segunda contribuição consiste em avaliar a *COBFE* mediante a utilização de filtros ópticos disponíveis na literatura. A terceira foi fazer essa avaliação para formatos de modulação avançados, respectivamente, para sinais modulados com *DPSK*, *DQPSK* e *16-QAM*. Também foram feitas simulações para avaliar relação sinal-ruído óptico e observar o comportamento da *COBFE* quanto o sinal é propagado. Alguns resultados deste trabalho foram publicados [29, 32, 33] e outros submetidos [34, 35].

1.4. Organização do trabalho

Este trabalho está organizado da seguinte maneira. O Capítulo 2 descreve a técnica de criptografia totalmente óptica avaliada neste trabalho. Neste mesmo capítulo, são feitas algumas comparações desta técnica com alguns trabalhos da literatura. Posteriormente é apresentado o arranjo usado nas simulações e, em seguida, são exibidos os perfis dos filtros utilizados. Nos Capítulos 3, 4 e 5, são abordados e discutidos os resultados das simulações para sinais *DPSK*, *DQPSK* e *16-QAM*. No Capítulo 6 são mostrados e discutidos

resultados de simulações dos sinais modulados com 16-QAM mediante a utilização de filtragem digital de *Nyquist* e filtros ópticos supergaussianos.

Finalizando, as conclusões deste trabalho são apresentadas no Capítulo 7.

2. CRIPTOGRAFIA ÓPTICA BASEADA EM FATIAMENTO ESPECTRAL – *COBFE*

Este capítulo descreve a *COBFE* avaliada neste trabalho. A Seção 2.1 apresenta a técnica. A Seção 2.2 mostra os filtros ópticos passa-faixa utilizados nas simulações. Na Seção 2.3 serão abordadas algumas comparações entre a *COBFE* e trabalhos relacionados. Finalizando o capítulo, a Seção 2.4 apresentará os arranjos das simulações.

2.1. Princípio da *COBFE*

A *COBFE* consiste em dividir o sinal óptico em n fatias espectrais. Essa divisão pode ser feita utilizando demultiplexadores ópticos, divisores ou qualquer dispositivo óptico capaz de dividir o sinal. Em seguida, o sinal de cada fatia passa por um Filtro Óptico Passa Banda (*Optical Band Pass Filter*, OBPF) alocando assim, a fatia espectral numa faixa de frequência determinada. Com relação ao sinal filtrado de cada fatia espectral, o posicionamento no domínio da frequência respeita um espaçamento entre filtros, denominado δ , como pode ser visto na Fig. 6.

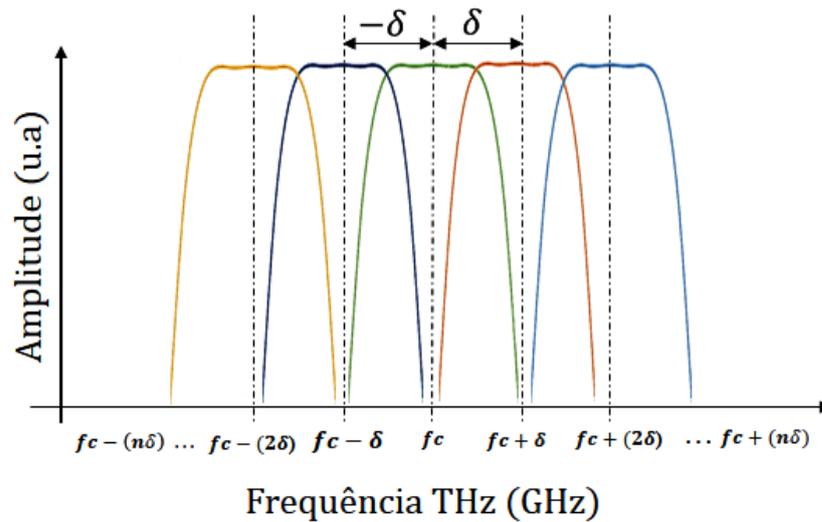


Figura 6 - Disposição dos filtros no domínio da frequência

Após a divisão do sinal, podem-se utilizar diferentes maneiras de efetuar a codificação. Em especial, neste trabalho são consideradas três e cada codificação é representada por um módulo.

O primeiro módulo consiste na codificação da amplitude e é denominado Codificação Espectral de Amplitude (*Spectral Amplitude Encoding, SAE*). No segundo a codificação é feita por atraso dos bits e é designada Codificação Espectral por Atraso (*Spectral Delay Encoding, SDE*). Por fim, o terceiro módulo realiza a codificação por desvio de fase, e este é chamado de Codificação de Fase Espectral (*Spectral Phase Encoding, SPE*). Estes módulos podem ser observados por intermédio da estrutura do codificador, ilustrada na Fig. 7.

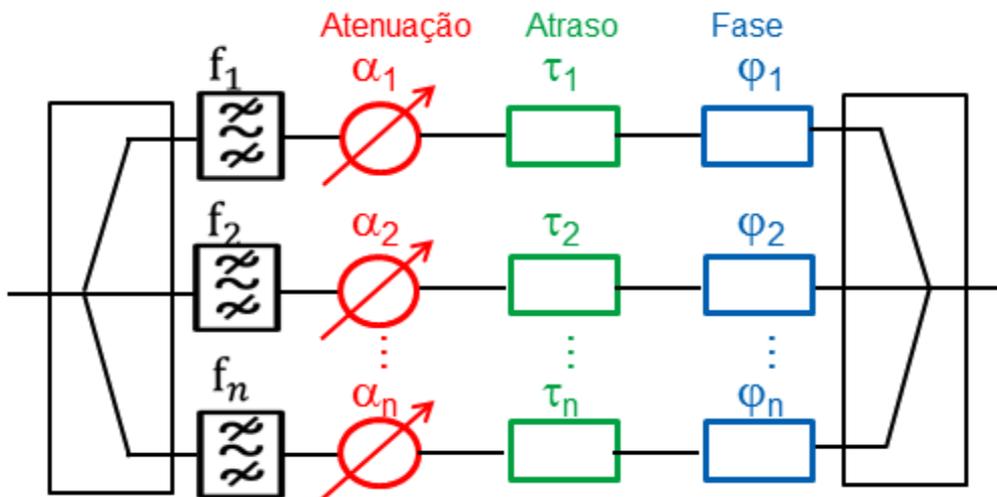


Figura 7 - Diagrama de bloco da técnica de codificação do sinal óptico

Uma vez que o sinal de cada fatia é filtrado, dá-se início ao processo de codificação por intermédio dos módulos, e estes, por sua vez, podem ser operados simultânea ou individualmente. Entretanto, por razões que serão apresentadas no Capítulo 6, este trabalho apresenta resultados para a técnica composta apenas pelos módulos *SDE* e *SPE*.

Na *SAE*, o sinal de cada fatia é submetido a uma dada atenuação, α_i . Assim, $\alpha_i (i = 1, 2, \dots, n)$ com a atenuação máxima representada pelo coeficiente $\alpha_{m\acute{a}x}$ [26, 27]. Outra possibilidade é a utilização do módulo da *SDE*. Neste módulo, o sinal de cada fatia é submetido a um dado atraso, τ_i , que pode variar na ordem de período de bits inteiros ou símbolos, T_b . Assim, com respeito às fatias, $\tau_i (i = 1, 2, \dots, n)$, e o maior desses atrasos é representado pelo coeficiente $\tau_{m\acute{a}x}$.

Analogamente ao atraso e a atenuação, pode-se utilizar somente o módulo da fase visando obter a *SPE*. Neste módulo, o sinal de cada fatia é submetido a um dado desvio de fase, φ_{ci} , que pode assumir qualquer valor

compreendido entre 0° a 360° . Todavia, por razões que serão apresentadas na Seção 3.1, as chaves criptográficas utilizadas para a codificação em fase estão no intervalo de 0° a 180° . Dessa forma, tem-se φ_i ($i = 1, 2, \dots, n$), com a fase máxima representada pelo coeficiente, $\varphi_{m\acute{a}x}$.

Após o processo de codificação, os sinais das fatias são acoplados ou multiplexados. Assim, na saída é obtida uma versão distorcida do sinal. Consequentemente, as informações contidas no sinal codificado, quando transmitidas em uma TON ou qualquer outro circuito óptico, são relativamente difíceis de serem detectadas por um intruso ou qualquer pessoa não autorizada.

Neste trabalho, um dos métodos usados para analisar a robustez da COBFE é a análise da taxa de erro de bits, (*Bits Error Rate*, BER) do sinal codificado (BER_c). Sendo assim, BER_c deve ser tão alta quanto possível. Neste trabalho, admite-se que o valor mínimo que ela deve ter é de 10%.

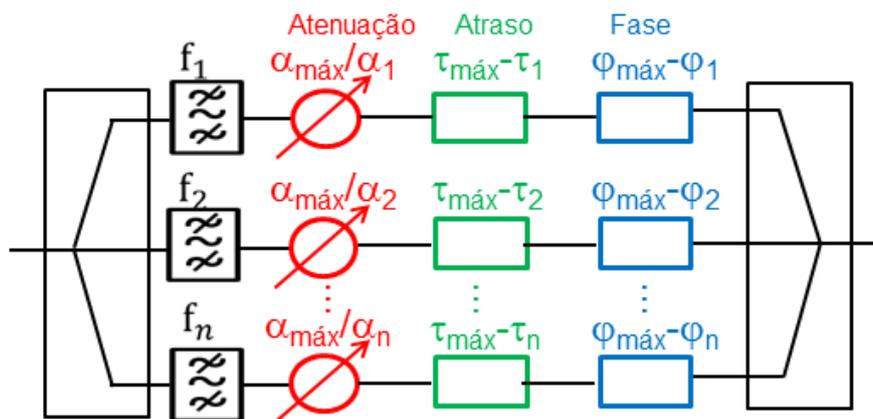


Figura 8 - Diagrama de bloco do decodificador óptico

A estrutura da figura 8 é utilizada para implementar o decodificador óptico da COBFE, neste por sua vez, o sinal é novamente dividido por intermédio de

splitters ou demultiplexadores ópticos. Dessa forma, para a recuperação de sinais codificados com *SAE*, as atenuações inseridas em cada fatia do codificador são compensadas no decodificador por meio da razão entre a atenuação máxima e a atenuação da fatia correspondente. Dessa forma, a atenuação para todas as fatias será

$$\alpha_{Di} = \frac{\alpha_{m\acute{a}x}}{\alpha_{Ci}} \quad (1)$$

em que $\alpha_{m\acute{a}x}$ representa a atenuação máxima estipulada, α_{Ci} diz respeito à atenuação no codificador para uma determinada fatia e, α_{Di} , a atenuação compensada no decodificador, respeitando (1).

Seguindo o mesmo princípio, a recuperação de sinais codificados com *SDE* é feita no decodificador por meio da subtração do atraso máximo pelo atraso inserido na respectiva fatia espectral. Sendo assim, pode-se verificar que

$$\tau_{Di} = \tau_{m\acute{a}x} - \tau_{Ci} \quad (2)$$

em que $\tau_{m\acute{a}x}$ corresponde ao atraso máximo, τ_{Ci} representa o atraso inserido em uma dada fatia no codificador e τ_{Di} representa o atraso compensado no decodificador, definido por (2).

Analogamente, a recuperação da *SPE* pode ser determinada por

$$\varphi_{Di} = 360^\circ - \theta_{Ci} \quad (3)$$

em que θ_i corresponde ao ângulo de incremento necessário para se completar 360° , tal como ilustra a Fig. 9. Assim, por exemplo, inserindo um desvio de fase

de 30° em uma dada fatia espectral no codificador, por (3) são necessários 330° no decodificador para se recuperar a fase desviada.

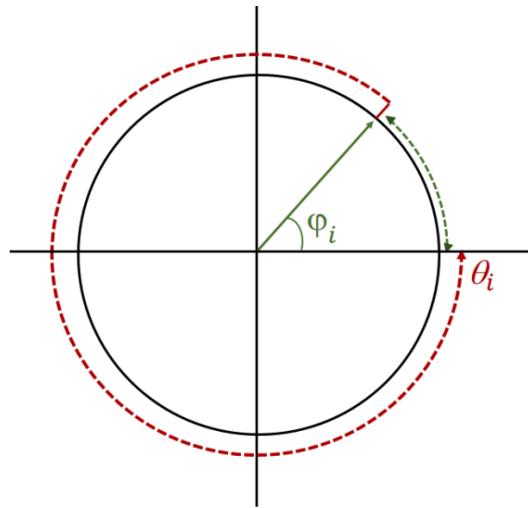


Figura 9 - Ciclo trigonométrico para a relação entre fase

Finalmente, o sinal é novamente recomposto, obtendo assim, uma versão do sinal sem distorção e decodificado, que idealmente apresenta BER_d inferior a 10^{-15} . Neste trabalho, convencionou-se que um chave óptica K é representada por $K = \{n, \alpha_1, \alpha_2, \dots, \alpha_n; \tau_1, \tau_2, \dots, \tau_n; \varphi_1, \varphi_2, \dots, \varphi_n\}$, em que $n, \alpha_i, \tau_i, \varphi_i$ foram definidas anteriormente como o número de fatias, atenuação, atraso e fase.

Uma maneira de aperfeiçoar a $COBFE$ é aumentando o número de fatias espectrais. Para que seja possível aumentar o número de fatias espectrais, ou seja, dividir ainda mais o sinal, são necessários $OBPF$'s com largura de banda estreita o suficiente para que essa divisão ocorra.

2.2. Arranjos das simulações *back-to-back*

As simulações da COBFE foram realizadas por intermédio do software *VPI Transmission Maker Optical Systems*, versão 9.1. Este software, por sua vez, foi instalado em um computador com o sistema operacional Windows 7 Pro 64 bits, 64 GB de memória RAM com um processador Intel (R) Xeon(R) CPU E5-2603 @ 1.80GHz.

A Fig. 10 apresenta o diagrama de bloco referente ao arranjo das simulações. Este arranjo pode assumir diferentes tipos de transmissores, porém, neste trabalho, foram usados *DPSK*, *DQPSK* e *16-QAM*, suas características são apresentadas na Tabela 1.

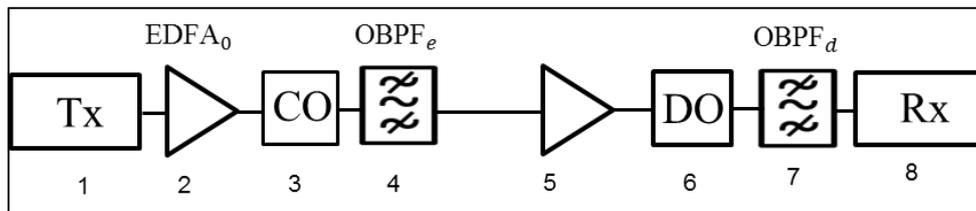


Figura 10 - Diagrama de bloco usado para simulações *back-to-back*

- 1 - Transmissor óptico
- 2 e 5 - Amplificador óptico à fibra dopada com érbio
- 3. Codificador óptico
- 4 e 7 - Filtro óptico passa banda
- 6 - Decodificador óptico
- 8 - Receptor óptico

Tabela 1 - Parâmetros utilizados nas simulações

Modulação	Taxa da transmissão (Gbps)	Quantidade de bits transmitidos	Frequência central (THz)	Potência do sinal transmitido	Banda do filtro (GHz)	Resolução espectral
DPSK	40	65436 (PRBS)	193,1	1 mW	14	0,5 GHz
DQPSK	40	65436 (PRBS)	193,1	1 mW	7,8	0,5 GHz
16-QAM	200	65436 (PRBS)	193,1	1 mW	30	0,5 GHz

Uma vez estabelecidos os parâmetros de cada tipo de modulação, de maneira geral, o arranjo funciona da seguinte maneira. Um transmissor óptico (Tx) envia um sinal modulado, que por sua vez, é enviado a um amplificador de fibra dopada com érbio ($EDFA_C$) onde a potência média é ajustada para 1 mW. Em seguida, o sinal é enviado ao codificador, descrito na seção 2.1, no qual o sinal é dividido em 7 fatias espectrais, cada fatia com banda definida pelos $OBPFs$ utilizados em cada modulação. Após isso, são atribuídos às fatias todos os parâmetros de codificação.

Prosseguindo com a técnica, após o sinal ser codificado, uma redução do ruído e obtenção de melhor eficiência espectral na modulação é feita por meio de um $OBPF_C$. Após filtrar o sinal, amplifica-se novamente o sinal, dessa vez com $EDFA_D$ para assegurar que a potência do sinal no decodificador seja igual a 1 mW. Finalmente, é feita novamente a redução de ruído por intermédio do $OBPF_D$. Em termos de detecção, tanto o sinal codificado como decodificado foram avaliados por intermédio de analisadores de sinal óptico, realizando análises no domínio do tempo e frequência.

2.3. Comparações entre a *COBFE* e trabalhos relacionados

Dentre os trabalhos relacionados, apresentados na seção 1.2, observa-se que [21] é o que mais se assemelha à *COBFE*. No entanto, é importante destacar algumas de suas diferenças com relação à *COBFE*. A técnica avaliada em [21] considera *OBPF* com largura de banda mais estreitas do que os disponíveis comercialmente, este não é o caso do presente trabalho, em que se assume a utilização de *OBPF* com largura de banda e perfil baseados em *OBPFs* que podem ser encontrados na literatura [36]. É importante destacar também que, a técnica apresentada em [21], utiliza somente codificação em fase que, por sua vez, é bastante determinística, visto que, para uma mesma sequência de bits a codificação é sempre a mesma. Já a *COBFE*, além da codificação em fase, utiliza também atrasos, τ_i , nas fatias como parte da chave criptográfica que, por sua vez, embaralham os bits independentemente da sequência transmitida.

Uma restrição tecnológica da *COBFE* em relação às outras, reside no fato da dependência de *OBPFs* comerciais com largura de banda relativamente estreita, visto que, como mencionado anteriormente, os *OBPFs* com largura de banda mais estreitas disponíveis atualmente no mercado são de 4 GHz. Por exemplo, um sinal de largura de banda de 40 GHz, pode ser dividido em, no máximo, dez fatias de 4 GHz cada.

2.4. Perfis dos *OBPF* utilizados

A Fig. 11 ilustra o perfil dos *OBPFs* utilizados nas simulações com sinas, (a) *DPSK*, (b) *DQPSK* e (c) 16-QAM. Estes filtros foram baseados em um *OBPF* de fotônica de silício apresentado na literatura inicialmente em [36]. Originalmente, este *OBPF* apresenta uma banda de 8 GHz, medida a 20 dB. Dependendo da necessidade, a largura de banda deste *OBPF* foi redimensionado para atender cada formato de modulação.

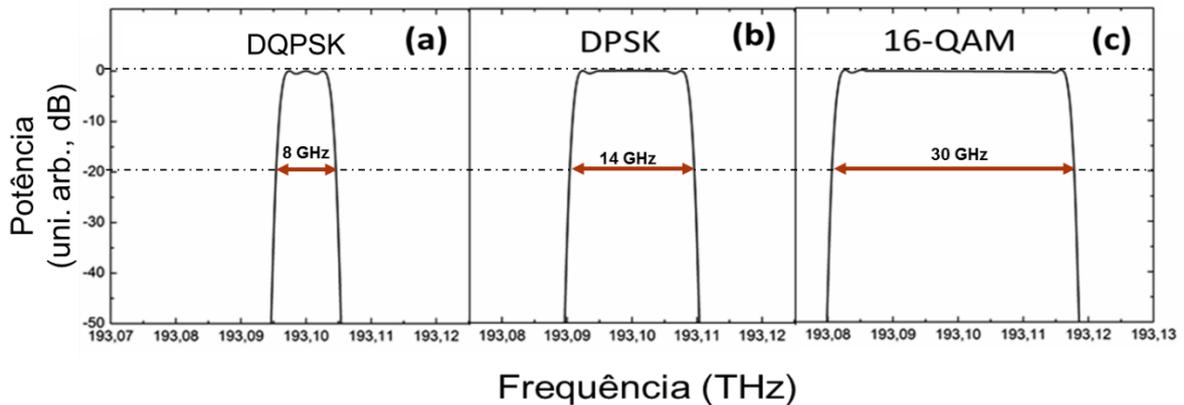


Figura 11 – Representação dos perfis dos filtros utilizados

Para as simulações com formato de modulação *DQPSK*, sobrepôs-se 4 filtros de modo a deixá-lo com a banda mais estreita obter uma largura de banda de 7 GHz. Esta banda se multiplicada pelo número de fatias espectrais atinge a banda desejada para estas simulações.

Nas simulações com sinais *DPSK*, mantiveram a mesmas configurações do filtro, no entanto, o *OBPF* foi redimensionado para uma banda de 14 GHz para que se pudesse atingir uma banda de 80 GHz, uma vez que, para este formato de modulação a taxa utilizada foi de 40 Gbps. Assim sendo, o mesmo

ocorreu nas simulações com formato de modulação 16-QAM, em que houve a necessidade de aumentar a largura de banda do *OBPF* para 30 GHz e assim realizar simulações com uma taxa de 200 Gbps.

3. ANÁLISE DOS RESULTADOS DAS SIMULAÇÕES DA COBFE PARA SINAIS DPSK

Este capítulo apresenta as análises dos resultados para as simulações com sinais *DPSK*. Na Seção 3.1 serão apresentados os resultados no domínio do tempo, além de análises dos diagramas de olho e das sequências de bits. Na Seção 3.2, serão apresentados os resultados no domínio da frequência, ou seja, os espectros ópticos. Posteriormente, na Seção 3.3, serão apresentados os resultados sobre a influência do atraso em BER_C em função da fatia espectral. Em seguida, a Seção 3.4 apresentará os resultados sobre a influência da fase em BER_C em função da fatia espectral. Por fim, na Seção 3.5, serão apresentados resultados da influência do número de fatias espectrais em BER_C em função da *OSNR*.

As simulações referentes aos resultados apresentados nessa seção foram realizadas de acordo com os parâmetros apresentados na Tabela 1, e a chave criptográfica utilizada é apresentada na Tabela 1, exceto quando mencionado de outra forma. No entanto, observa-se que este é apenas um exemplo de chave e que a *COBFE* funciona com outras chaves. Nas simulações referentes aos resultados apresentados nesta seção, foi utilizada a seguinte chave criptográfica: $k=\{7, \tau_1 =250, \tau_2 =75, \tau_3 =225, \tau_4 =250, \tau_5 =200, \tau_6 =10, \tau_7 =100; \varphi_1 =30, \varphi_2 =110, \varphi_3 =170, \varphi_4 =260, \varphi_5 =80, \varphi_6 =180, \varphi_7 =150\}$. Na qual todos os atrasos estão indicados em picossegundos e as fases em grau. Vale realçar que a técnica funciona para diferentes chaves.

3.1. Análise dos resultados nos domínios do tempo e da frequência

3.1.1. Sequências temporais

A Fig. 12 ilustra as representações das sequências de bits dos sinais, (a) gerado pelo transmissor, (b) codificado e (c) decodificado. Neste trabalho, admite-se que todos os sinais que representam os bits com a potência máxima superior ao nível médio do sinal são considerados como bits 1 e que aqueles que tiverem potência máxima inferior ao nível médio do sinal são considerados bits 0.

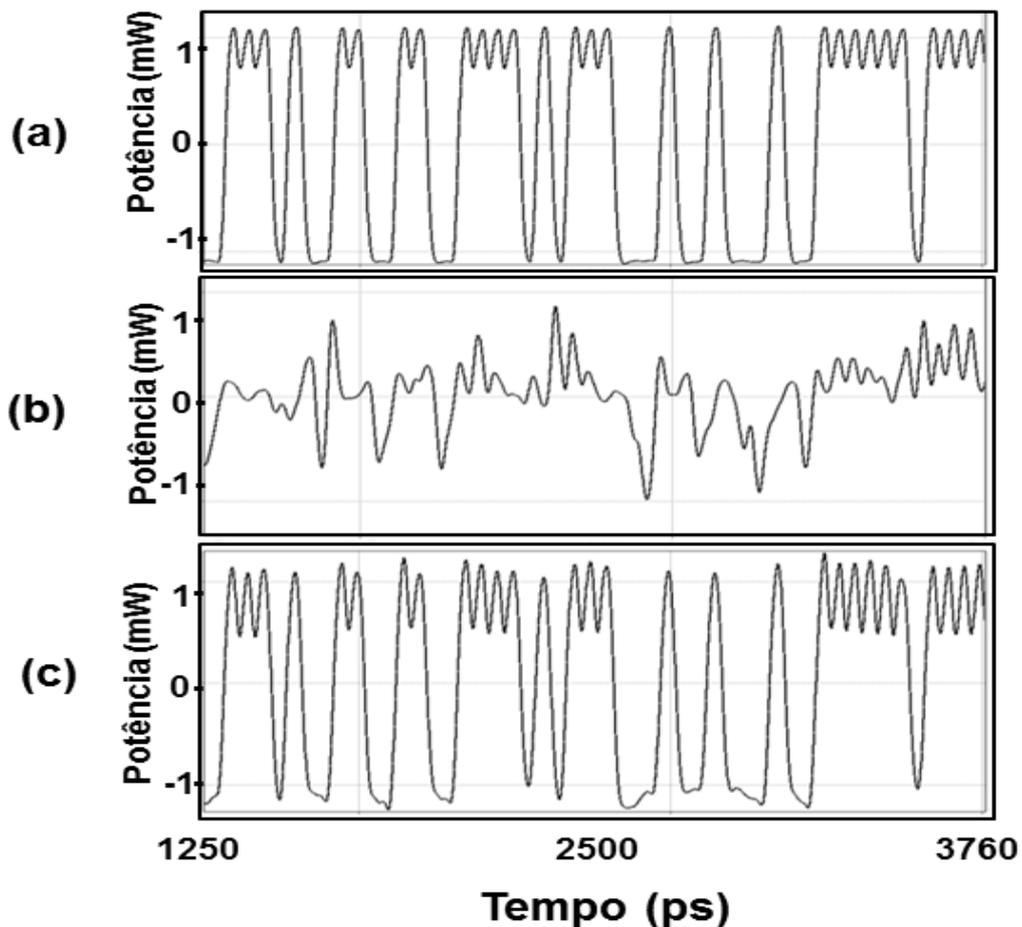


Figura 12 - representações das sequências de bits dos sinais, (a) gerado pelo transmissor, (b) codificado e (c) decodificado

Tendo em conta que o propósito da *COBFE* é a degradação artificial do sinal, é de extrema importância que BER_C seja sempre maior que o limite de BER da FEC (neste trabalho admitido como $BER_{FEC} 10^{-3}$). Dado o limite de BER_{FEC} , foi estabelecido um critério em que BER da criptográfica do sinal (BER_{CRI}) deve ser sempre, no mínimo, cem vezes maior que o limite de BER_{FEC} , ou seja, $BER_{CRI} = 100BER_{FEC}$.

A representação da sequência de bits do sinal gerado pelo transmissor, ilustrada na Fig. 12 (a), é usada como referência, e esta não apresenta nenhum bit errado. Por outro lado, a representação da sequência de bits do sinal codificado, ilustrada na Fig. 12 (b), apresenta um número relativamente elevado de bits errados. Deste modo, a detecção do sinal codificado torna-se uma tarefa relativamente difícil para alguém que desconhece a técnica. De fato, os resultados das simulações indicam que BER_C associada à Fig. 12 (b) é estimada em 10% (dentro do limite estabelecido).

Diferente do sinal codificado, a representação da sequência de bits do sinal decodificado, ilustrada na Fig. 12 (c), muito embora esta tenha apresentado algumas variações nos níveis de potência dos bits, tais variações não foram suficientes para degradar o sinal e, conseqüentemente, não apresentou nenhum bit errado. Assim sendo, se comparadas às figuras 12 (a) e 12 (c), é relativamente fácil perceber que elas se assemelham muito. Resultados referentes a essa simulação indicam que BER_D associada a Fig. 12 (c) é inferior a 10^{-15} .

3.1.2. Diagramas de olho

A Fig. 8 apresenta os diagramas de olho dos sinais, (a) gerado pelo transmissor, (b) codificado e (c) decodificado. Estes diagramas de olho são referentes às representações das sequências de bits ilustradas na Fig. 7.

Observa-se que, o diagrama de olho gerado pelo transmissor não apresenta variação nos níveis de amplitude. Este fator contribui para um diagrama de olho sem distorção, o que implica em um sinal sem degradação e livre de erros de bits ($BER_d < 10^{-15}$).

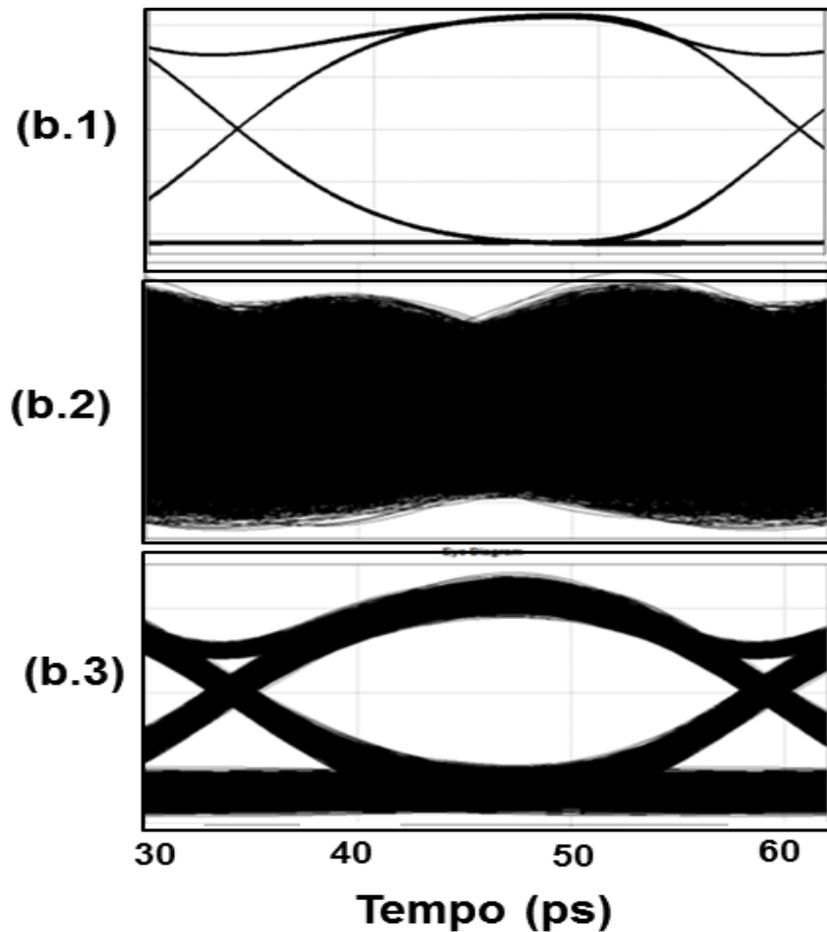


Figura 8- Diagramas de olho dos sinais, (a) gerado pelo transmissor, (b) codificado e (c) decodificado.

O diagrama de olho do sinal codificado, ilustrado na Fig. 8 (b), é referente à representação da sequência de bit ilustrada na Fig. 7 (b). É de fácil percepção que este está totalmente fechado e apresenta distorções resultantes de um sinal relativamente degradado. Lembrando que, resultados referentes a essas simulações indicam que BER é 10%.

Por outro lado, o diagrama de olho do sinal decodificado, ilustrado na Fig. 8 (c), é referente à representação da sequência de bits, ilustrada na Fig. 7 (a). Este apresenta pequenas distorções causadas pelo conjunto de filtros, porém, tais distorções não são suficientes para degradar o sinal, visto que, este também assemelha-se muito ao diagrama de olho do sinal gerado pelo transmissor (Fig. 8 a).

3.1.3. Espectros ópticos

Em seções anteriores foram apresentados os resultados no domínio do tempo (representações das sequências de bits e diagramas de olho). Neles, foi possível verificar distorções resultantes da degradação artificial do sinal.

Diferente dos dois casos anteriores, os espectros ópticos ilustrados na Fig. 13, (a) gerado pelo transmissor, (b) codificado e (c) decodificado, não apresentam distorções significativas. Isto ocorre, muito embora o sinal codificado esteja degradado pela *COBFE*, o que, por conseguinte, não permite que um intruso ou qualquer pessoa não autorizada identifique as alterações através do perfil espectral.

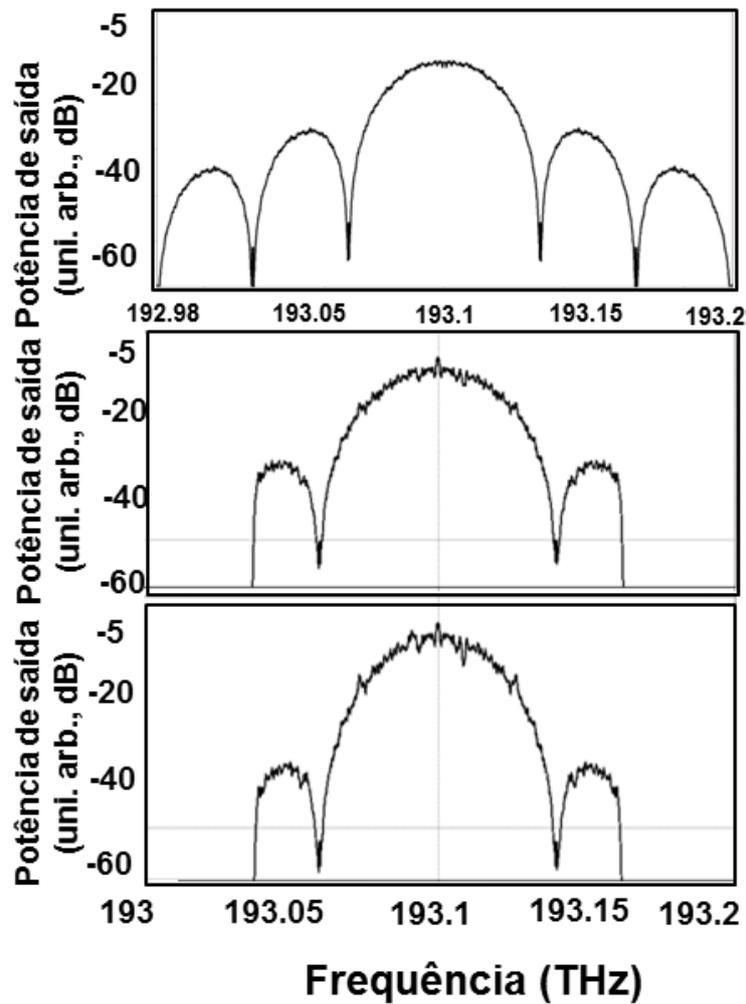


Figura 13 - Espectros óptico dos sinais, (a) transmitido, (b) codificado e (c) Decodificado

3.2. Influência do atraso na taxa de erro de bits do sinal codificado em função da fatia espectral

Foram realizadas simulações para avaliar a influência do atraso em BER_C . Nestas simulações, todas as fases das fatias foram igualadas a zero (sem codificação em fase) e a codificação por atraso foi feita, individualmente, em cada uma das fatias. Por exemplo, variou-se τ_1 de 25 a 250 ps, mantendo-se $\tau_i = 0$, para $i = (2$ a $7)$. Após isso, τ_2 foi variado e

manteve-se $\tau_i = 0$, para $i = 1$ e $i = (3 \text{ a } 7)$. Os resultados obtidos estão apresentados na Fig. 14.

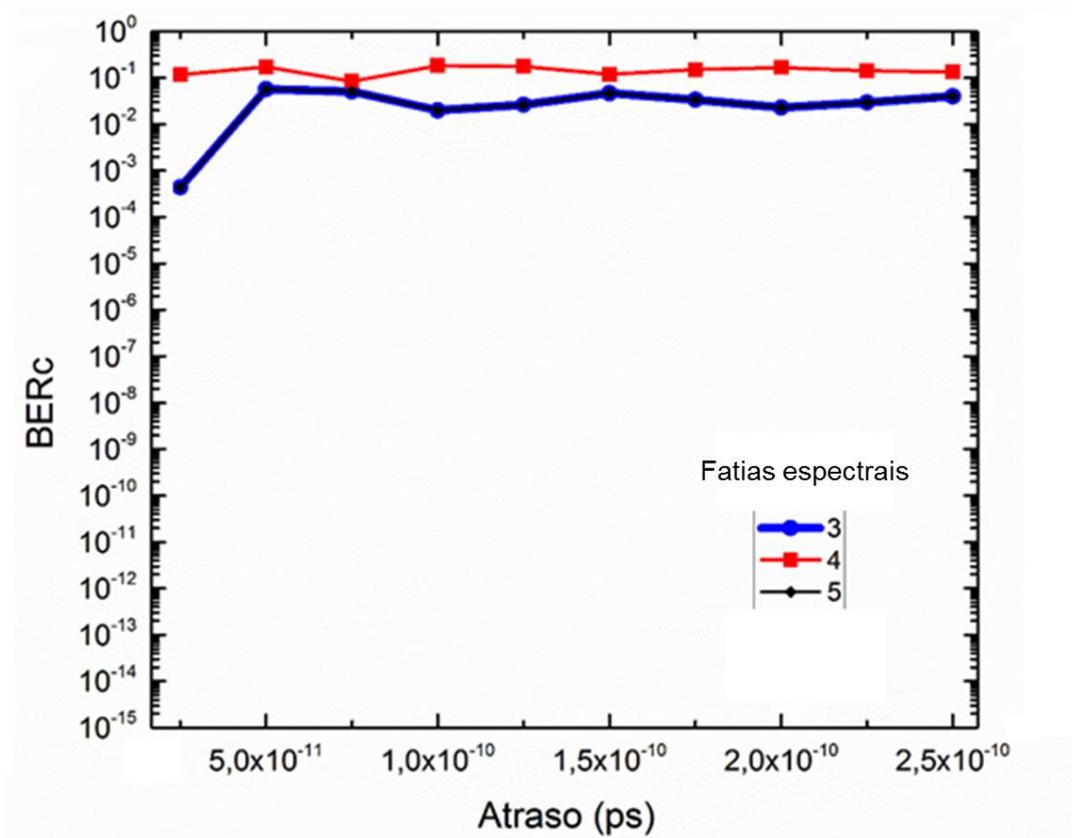


Figura 14 - Influência do atraso em BER_C em função das fatias espectrais

Como ilustra a Figura 9, BER_C foi de aproximadamente 10^{-1} , em todo intervalo de 25 a 250 ps, para o caso em que a codificação é realizada apenas na fatia central (apenas τ_4 variando). Este valor relativamente alto em BER_C ocorre porque a fatia central contém uma energia maior que as demais.

As fatias 3 e 5 são adjacentes à fatia 4 e estão opostamente deslocadas em frequência, em relação a esta. Por esta razão, a Fig. 14 mostra que a codificação apenas em τ_3 ou τ_5 conduzem aos mesmos valores de BER_C e que estes valores são inferiores àqueles obtidos quando a fatia 4 (que contém maior energia) é codificada. De fato, nota-se que com um atraso de 25 ps, BER_C foi de

aproximadamente 10^{-3} . No intervalo analisado, BER_C varia entre $\sim 5 \cdot 10^{-4}$ e $1 \cdot 10^{-1}$.

As curvas para variações de τ_1 , τ_2 , τ_6 e τ_7 não estão indicadas na Fig. 14 porque todas apresentam BER_C inferior a 10^{-15} . No entanto, é interessante notar que, resultados de simulações de outros trabalhos indicam que a codificação simultânea de várias fatias pode aumentar BER_C .

3.3. Influência da fase na taxa de erro de bits do sinal codificado em função da fatia espectral

Analogamente ao caso anterior (Seção 3.2), um estudo da variação da fase foi realizado visando a analisar sua influência em BER_C para todas as fatias de maneira individual, tal como pode ser visto na Fig. 15. Assim sendo, estabeleceu-se a seguinte metodologia, primeiramente, variou-se a fase para uma dada fatia, por exemplo, item (a), e atribui-se fases iguais a 0° para as demais, item (b).

a) φ_1 variando de 0° a 360°

b) $\varphi_2, \varphi_3, \varphi_4, \varphi_5, \varphi_6, \varphi_7 = 0^\circ$

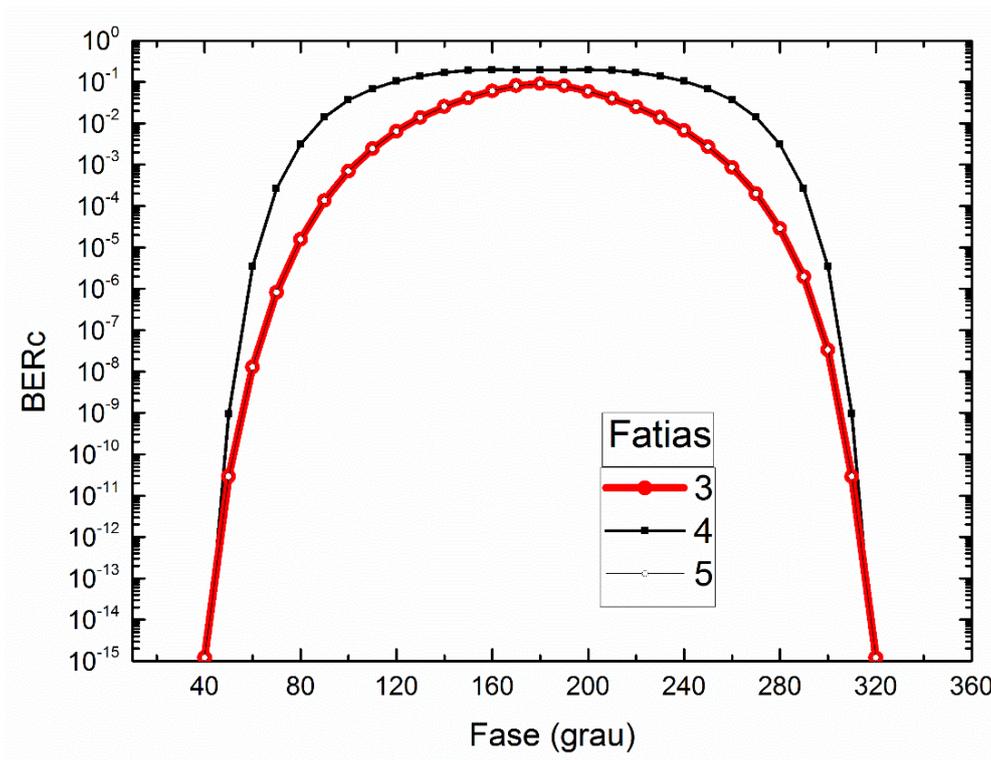


Figura 15 - Influência da fase na BER_c em função da fatia espectral

Em resultados anteriores (Seção 3.2), observou-se que com a variação do atraso, a codificação é mais significativa na fatia central (fatia 4, atraso φ_4). Novamente, tal comportamento também é observado na codificação em fase. Tal fato se dá, novamente, devido a fatia central conter maior parte da energia do sinal.

Ainda nesse sentido, as fatias 3 e 5 (fases φ_3 e φ_5), novamente, por serem adjacentes à fatia 4 e estarem igualmente deslocadas em frequência, apresentam comportamento relativamente análogo à fatia central. Todavia, estas apresentam BER_C inferiores à obtida na fatia 4. Dessa maneira, conclui-se que as codificações nessas fatias exercem menor influência se comparadas com a fatia central (fatia 4).

Seguindo a mesma linha de raciocínio para as fatias adjacentes, as fatias 1, 2, 6 e 7 (fases φ_1 , φ_2 , φ_6 e φ_7) contêm energia muito menor que a das outras fatias, isso implica em menor influência em BER_c . A codificação para cada uma dessas fatias apresentou BER_c inferior a 10^{-15} . Por esta razão, suas curvas não são ilustradas no gráfico.

Ainda na figura 15, pode-se observar que as curvas do gráfico são simétricas em relação ao eixo vertical na posição de 180° no eixo X, isto é, $BER(\theta) = BER(-\theta)$. Sendo assim, a utilização da codificação em fase com até 180° ou superior, é de caráter opcional, visto que, para os dois casos é possível obter o mesmo desempenho na codificação do sinal.

3.4. Influência do número e posição das fatias espectrais na taxa de erro de bits do sinal decodificado em função da relação sinal-ruído óptica

A relação sinal ruído óptica (*Optical Signal-To-Noise Ratio, OSNR*) é um dos parâmetros usados neste trabalho para avaliar o desempenho da COBFE. O desempenho da codificação do sinal depende dos parâmetros da COBFE e também da OSNR do sinal recebido. Por esta razão, é importante avaliar o comportamento de BER_D em função da OSNR. Para fazer tal avaliação, foram realizadas simulações baseadas no arranjo descrito na Fig. 10, mas incluindo ruído entre o transmissor e o receptor.

A Figura 16 ilustra os resultados de BER_D em função da OSNR. Supondo que um receptor não autorizado conheça apenas os parâmetros de codificação de uma ou mais fatias espectrais. Por exemplo, a linha vermelha ilustra o caso em que um intruso ou receptor não autorizado conhece os parâmetros de

codificação apenas da fatia 4. A linha azul, ilustra a situação em que o intruso conhece os parâmetros de codificação das fatias 4 e 5. Assim por diante até o caso em que o intruso conhece os parâmetros de codificação de todas as fatias.

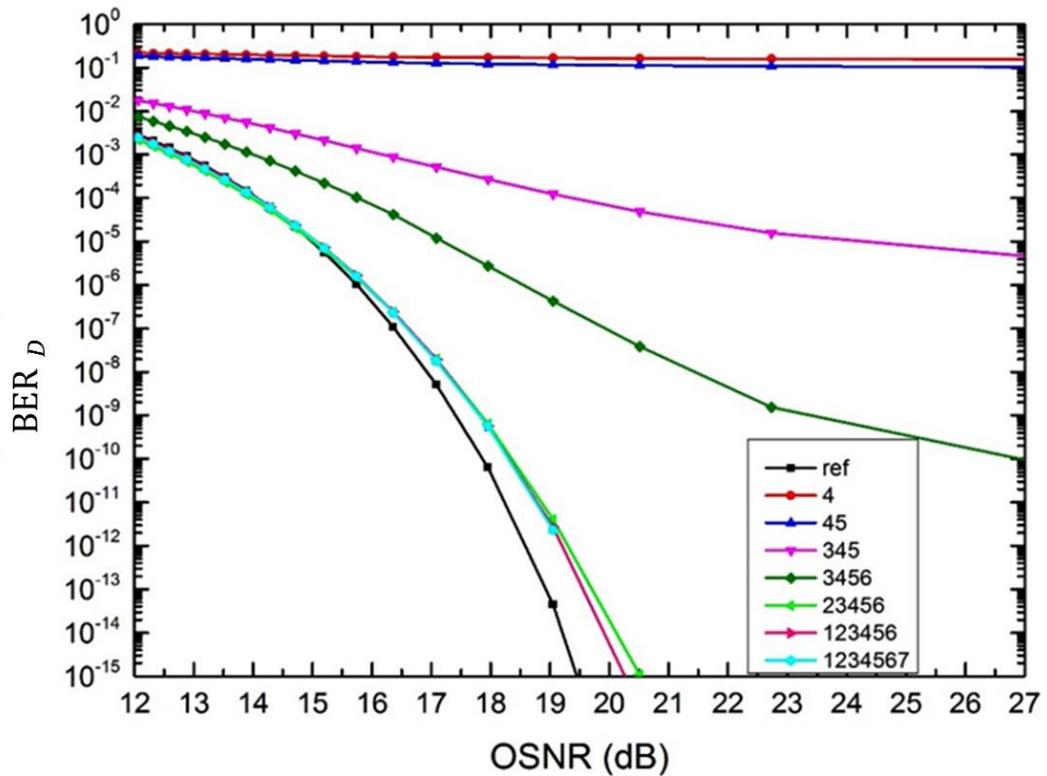


Figura 16 - Gráfico Influência do número e posição das fatias espectrais em BER em função da OSNR

Nesta mesma figura, observa-se que, para que um intruso consiga recuperar o sinal, o mesmo precisa conhecer os parâmetros de exatamente quatro fatias que contêm maior energia e obter BER_D de 10^{-3} com 14 dB de OSNR. Caso OSNR seja de 16 dB, o intruso precisaria conhecer os parâmetros de codificação de apenas três fatias para obter uma BER_D de 10^{-3} .

4. ANÁLISE DOS RESULTADOS DAS SIMULAÇÕES DA COBFE PARA SINAIS *DQPSK*

Neste capítulo, serão apresentados os resultados das simulações da COBFE com a modulação *DQPSK*. Na Seção 4.1 serão apresentados os resultados no domínio do tempo, além de análises das sequências de bits e dos diagramas de olho. Na Seção 4.2, serão apresentados os resultados no domínio da frequência, ou seja, os espectros ópticos. Posteriormente, na Seção 4.3, serão apresentados os resultados sobre a influência do atraso em BER_C em função da fatia espectral. Em seguida, a Seção 4.4 apresentará os resultados sobre a influência da fase em BER_C em função da fatia espectral. Por fim, na Seção 4.5, serão apresentados resultados sobre a influência do número de fatias espectrais em BER_C em função da $OSNR$.

De igual modo às simulações com sinais *DPSK*, as simulações para modulação *DQPSK* também foram realizadas de acordo com os parâmetros encontrados na Tabela 1. A chave criptográfica usada nas simulações para esta modulação foi: $K = \{7, \tau_1 = 250, \tau_2 = 150, \tau_3 = 50, \tau_4 = 255, \tau_5 = 100, \tau_6 = 125, \tau_7 = 50; \varphi_1 = 30, \varphi_2 = 90, \varphi_3 = 140, \varphi_4 = 65, \varphi_5 = 130, \varphi_6 = 115, \varphi_7 = 160\}$. Em que os atrasos estão indicados em picossegundos e as fases em grau.

4.1. Análise dos resultados nos domínios do tempo e da frequência

4.1.1. Sequências temporais

A Fig. 17 ilustra as representações das sequências de bits dos sinais, (a) gerado pelo transmissor, (b) codificado e (c) decodificado. Os resultados representados nestas figuras são analisados de acordo com os critérios adotados na Seção 3.1.1.

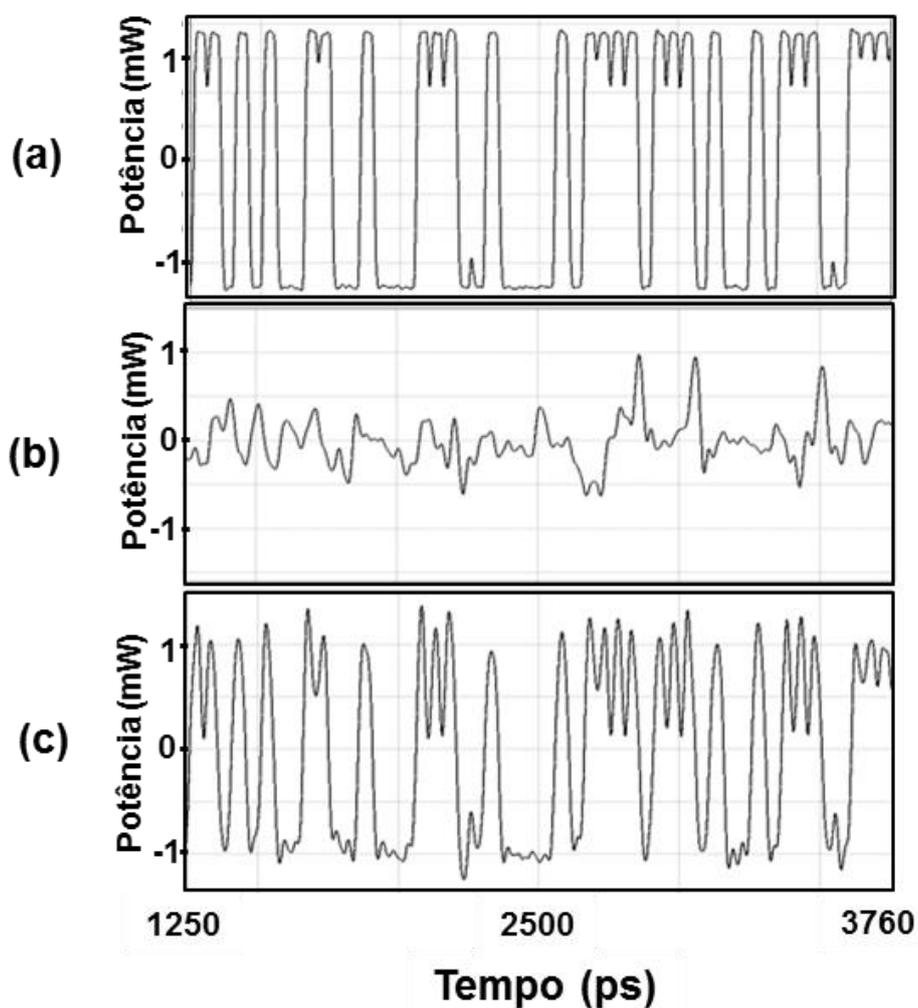


Figura 17 - Representações das sequências de bits dos sinais, (a) gerado pelo transmissor, (b) codificado e (c) decodificado.

Tal como na seção anterior, (3.1.1), a representação da sequência de bits do sinal gerado pelo transmissor, ilustrada na Fig. 17 (a), é usada como referência e representa um sinal sem degradação, ou seja, livre de erro de bits. Por outro lado, a Fig. 17 (b) representa a sequência de bits referente ao sinal codificado, que representa uma versão distorcida do sinal gerado pelo transmissor.

Ainda na Fig. 17, item (b), verifica-se que os bits estão embaralhados. Isso ocorre devido aos diferentes atrasos nos períodos dos bits e aos desvios de fase que constituem *COBFE*. Resultados de simulação indicam que BER_C associada a esta figura é estimada em 29 %.

Nota-se que, resultados de simulações apresentados na Seção 3.11, indicaram que BER_C associada à representação da sequência de bits do sinal *DPSK* codificado, ilustrada na Fig. 15 (b), foi de 10%. Estes resultados sugerem um desempenho inferior na codificação deste sinal se comparado com os resultados representados na Fig. 17 (b), em que BER_C é de 29 %.

Ainda neste contexto, o melhor desempenho da *COBFE* em sinais *DQPSK* em relação aos sinais *DPSK*, deve-se, novamente, ao fato de que as simulações para sinais modulados com *DQPSK* terem sido realizadas com *OBPFs* com largura de banda de 8 GHz e as simulações para sinais *DPSK* terem sido realizadas com *OBPFs* com largura de banda de 14 GHz. Além destes, o formato espectral de cada modulação pode interferir no desempenho da *COBFE*.

Observando a Fig. 17 (c) percebe-se que a representação da sequência de bits do sinal decodificado, se assemelha à gerada pelo transmissor. Apesar

de algumas variações nos níveis potência dos bits, resultados de simulações indicam que BER_D associada a esta representação é inferior a 10^{-15} .

4.1.2. Diagramas de olho

A Fig. 18 apresenta os diagramas de olho referentes aos sinais, (a) gerado pelo transmissor, (b) codificado e (c) decodificado. Os resultados representados nesta figura são relativos aos representados na Fig. 17. Por exemplo, a Fig. 18 (a) é referente à Fig. 17 (a), e assim sucessivamente. O diagrama de olho da Fig.18 (a), por este ser referente à sequência de bits representada na Fig. 17 (a), também é usado como referência, visto que, este é considerado livre de erros de bits. Por outro lado, o diagrama de olho do sinal codificado, ilustrado na Fig. 18 (b), apresenta-se totalmente fechado e distorcido. Este, por sua vez, representa uma versão degradada do sinal original. Desta maneira, torna-se relativamente indetectável por qualquer receptor não autorizado.

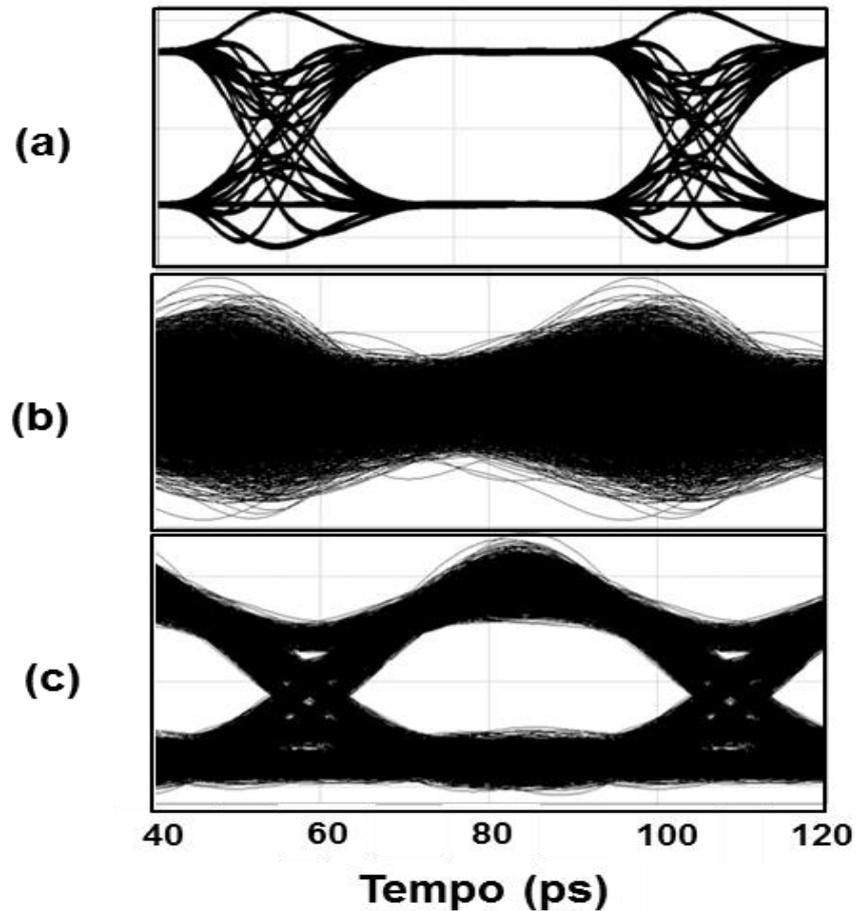


Figura 18 - Diagramas de olho dos sinais, (a) gerado pelo transmissor, (b) codificado e (c) decodificado.

Na Fig. 18(c), observa-se que o diagrama de olho referente ao sinal decodificado, apesar de apresentar pequenas variações nos níveis de amplitude (causadas pelos *OBPFs*), a ordem de grandeza destas variações não são suficientes para degradar o sinal. Assim, estes resultados corroboram com os resultados apresentados na Seção 3.1.2, (Fig. 17 c), em que o sinal decodificado se assemelha também ao sinal gerado pelo transmissor.

4.1.3. Espectros ópticos

A Fig. 19 apresenta os espectros ópticos dos sinais, (a) gerado pelo transmissor, (b) codificado e (c) decodificado. Tal como os resultados apresentados na Seção 3.1.1, nos espectros do sinal *DQPSK* também é possível constatar, por intermédio da Fig. 19 (b) que, apesar de a *COBFE* dividir o sinal em diversas fatias espectrais e este possuir BER_C relativamente elevada, estes espectros não apresentaram distorções significativas nos seus perfis que pudessem interferir negativamente no desempenho da *COBFE*. Vale salientar que resultados de simulações anteriores indicaram que BER_C associada a este sinal é estimada em 29%

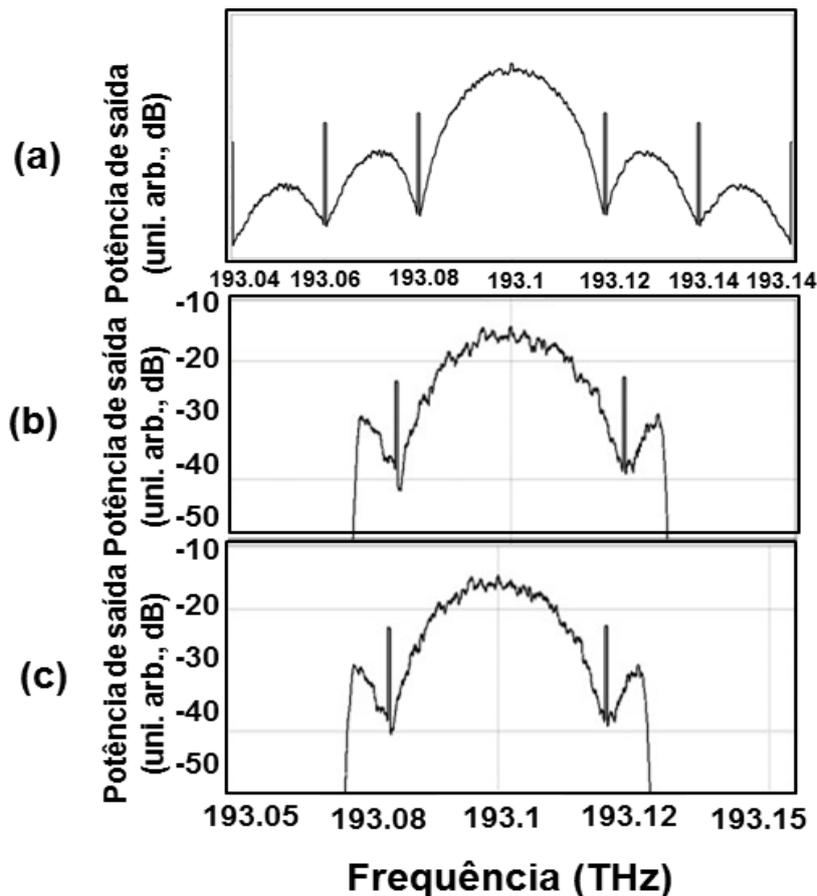


Figura 19 - Espectros ópticos dos sinais *DQPSK* transmitido, (b) Sinal codificado, (c) Sinal decodificado.

4.2. Influência do atraso na taxa de erro de bits do sinal codificado em função da fatia espectral

Foram realizadas simulações para avaliar a influência do atraso em BER_C . Estas simulações, por sua vez, foram realizadas utilizando a mesma metodologia e critérios apresentados na Seção 3.2. Nesta metodologia, para todas as fatias, as fases foram igualadas a zero (sem codificação em fase) e a codificação por atraso também foi feita, individualmente, em cada uma destas fatias. Por exemplo, variou-se τ_1 de 25 a 250 ps, mantendo-se $\tau_i = 0$, para $i = (2 \text{ a } 7)$. Após isso, τ_2 foi variado e manteve-se $\tau_i = 0$, para $i = 1$ e $i = (3 \text{ a } 7)$.

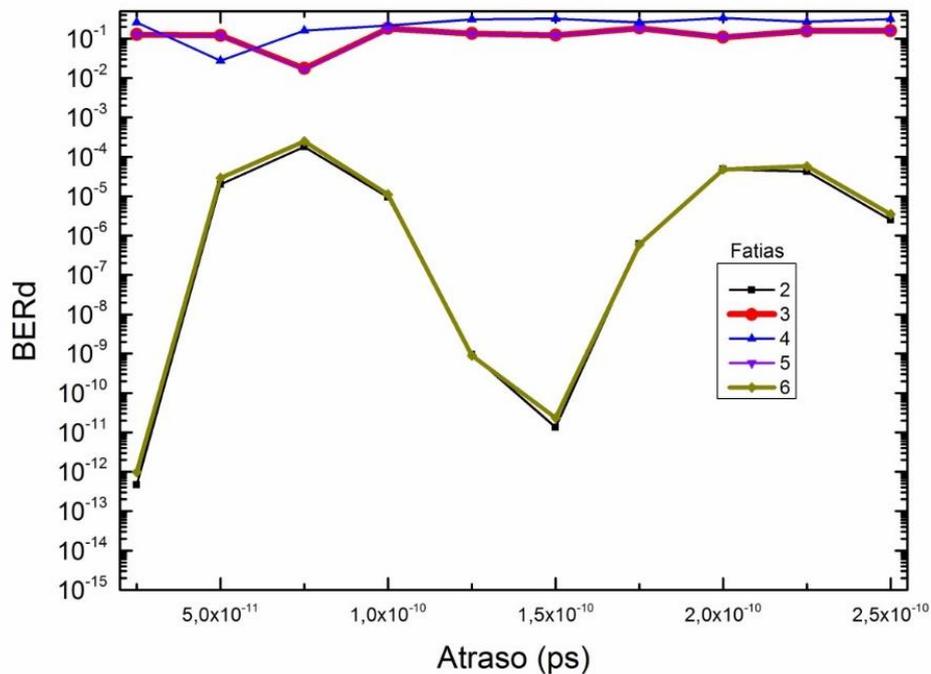


Figura 20 - Influência do atraso em BER_C em função da fatia espectral

Como ilustra a Figura 20, para o caso em que a codificação é realizada apenas na fatia central (apenas τ_4 variando), no intervalo de 25 a 250 ps, BER_C

foi de aproximadamente 10^{-1} . Este resultado se assemelha ao obtido em sinais DPSK para o mesmo intervalo (25 a 250 ps).

A mesma figura mostra também que, diferente dos resultados apresentados na Seção 3.2, na modulação *DQPSK*, a codificação apenas em τ_3 ou τ_5 , para o mesmo intervalo, BER_C varia entre $\sim 1 \cdot 10^{-2}$ e $1 \cdot 10^{-1}$ e com a codificação apenas em τ_2 ou τ_6 , BER_C varia entre $\sim 1 \cdot 10^{-12}$ e $1 \cdot 10^{-4}$. Tal fato deve-se, tal como em resultados apresentados em seções anteriores, pela utilização de *OBPFs* com largura de banda menor, isto é, *OBPFs* de 8 GHz de banda. Visto que, simulações com a modulação *DQPSK* foram realizadas com *OBPFs* de largura de banda de 14 GHz.

4.3. Influência da fase na taxa de erro de bits do sinal codificado em função da fatia espectral

Analogamente ao caso apresentado na Seção 3.3, um estudo da variação da fase em função da fatia espectral foi realizado visando analisar sua influência em BER_C para todas as fatias de maneira individual. Os resultados referentes a este estudo podem ser vistos na Fig. 21. Assim sendo, a metodologia utilizada na Seção 3.3, também foi utilizada para a realização deste estudo, bem como os critérios adotados para análise dos resultados.

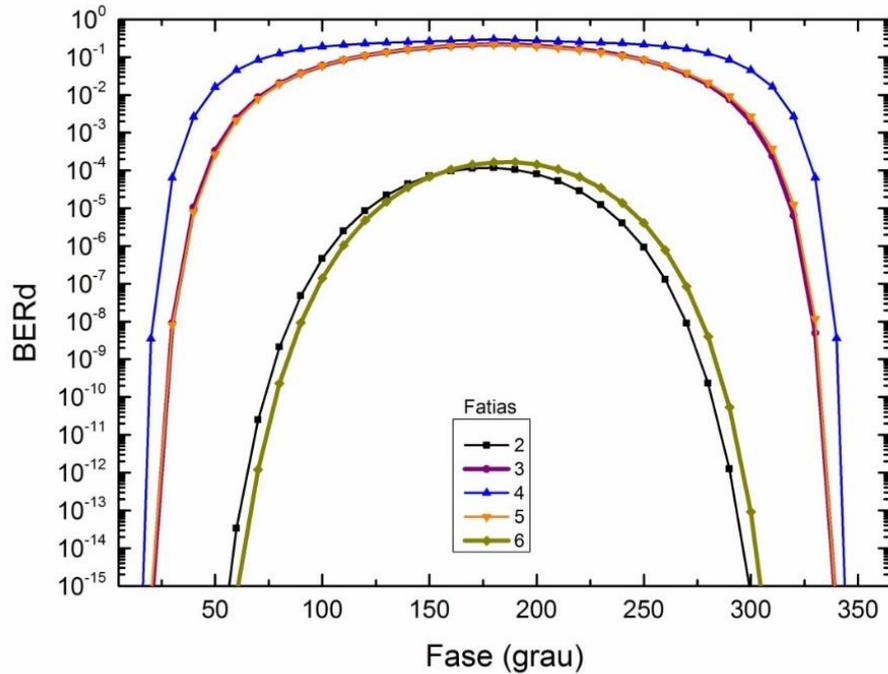


Figura 21 - Influência da fase na BER_C em função da fatia espectral

Na figura 21, constata-se que as curvas referentes às codificações nas fatias 3 e 5, no intervalo de 100 a 280 graus, BER_C é de aproximadamente 10^{-2} e apresentam comportamento relativamente análogo ao da fatia 4 (fatia central). No entanto, a fatia 4 apresenta BER_C de aproximadamente 10^{-1} para o intervalos de 75 a 300 graus. Lembrando que, tal comportamento também foi observado em resultados referentes à modulação *DPSK* (Seção 3. 3).

Outro ponto importante a observar neste mesmo gráfico (Fig. 21), é que, diferente dos resultados apresentados na Fig. 15, neste há presença das curvas referentes às fatias 2 e 6 e as curvas referentes às fatias 1 e 7 apresentaram BER_C inferior a 10^{-15} e, como nos casos anteriores, suas curvas não são ilustradas no gráfico. É importante destacar que, tal como indicam resultados de simulações anteriores, a diferença de desempenho da codificação de uma

modulação para outra pode depender de vários fatores. Em especial, nestas simulações o desempenho depende muito da largura de banda dos *OBPFs*.

4.4. Influência do número e posição das fatias espectrais na taxa de erro de bits do sinal decodificado em função da relação sinal-ruído óptica

Foram realizadas simulação para avaliar a influência do número e posição das fatias espectrais em BER_C em função da $OSNR$. Os resultados referentes a essas simulações são apresentados na Fig. 22.

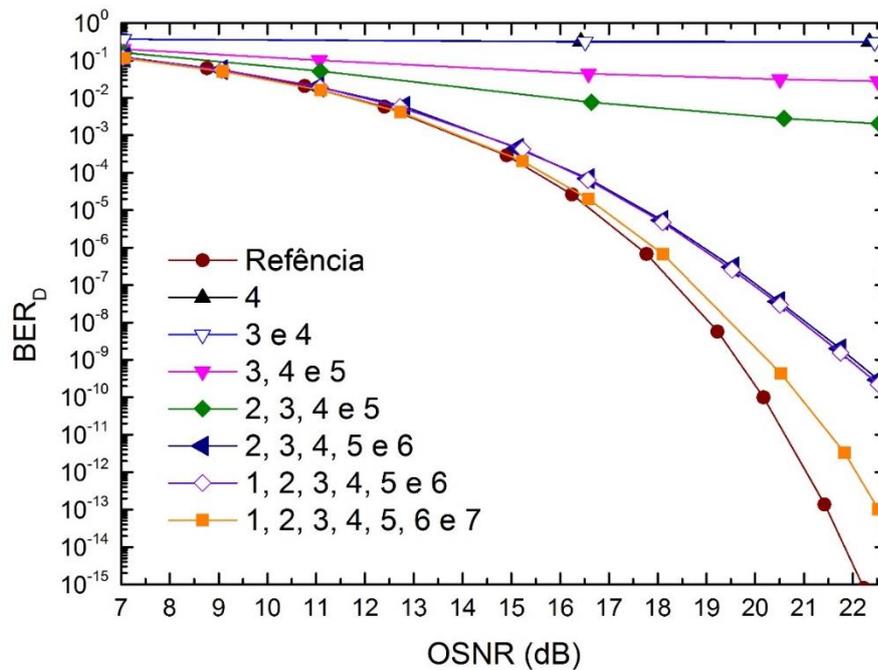


Figura 22 - Influência do número e posição das fatias espectrais na BER em função da OSNR

Seguindo a mesma linha de raciocínio apresentada na Seção 3.4, as curvas do gráfico (Fig. 22) mostram que, para que um intruso consiga recuperar o sinal por intermédio da *FEC*, o mesmo precisaria conhecer os parâmetros de quatro fatias e obter BER_D de 10^{-3} com 22 dB de $OSNR$.

Vele lembrar que, em resultados referentes à modulação *DPSK*, para que o intruso conseguisse BER_c de 10^{-3} , o mesmo precisaria conhecer parâmetros de apenas 4 fatias com 14 dB de *OSNR*. Estes resultados sugerem um melhor desempenho da *COBFE* em sinais *DQPSK* do que *DPSK*, isto devido a fatores já mencionados, como tipo de modulação e banda dos filtros ópticos utilizados.

5. ANÁLISE DOS RESULTADOS DAS SIMULAÇÕES DA COBFE PARA SINAIS 16-QAM

Em capítulos anteriores, foram apresentados resultados referentes às simulações para a modulação *DPSK* e *DQPSK*. Neste capítulo, serão apresentados os resultados das simulações para a modulação *16-QAM*. Na Seção 5.1 serão apresentadas as análises dos diagramas de constelações. Em seguida, na Seção 5.2 serão apresentadas as análises dos espectros ópticos. Posteriormente, na Seção 5.3 serão apresentados os resultados sobre a influência do atraso em BER_C em função da fatia espectral. Na Seção 5.4 serão apresentados os resultados sobre a influência da fase em BER_C em função da fatia espectral. Finalizando o capítulo, na Seção 5.5 serão apresentados os resultados das simulações sobre a influência do número e posição das fatias espectrais em BER_C em função da *OSNR*.

Analogamente às simulações com modulações *DPSK* e *DQPSK*, as simulações com a modulação *16-QAM* também foram realizadas de acordo com os parâmetros encontrados na Tabela 1. Para estas simulações, a chave utilizada foi: $k = \{7, \tau_1 = 50, \tau_2 = 15, \tau_3 = 20, \tau_4 = 45, \tau_5 = 30, \tau_6 = 10, \tau_7 = 35; \varphi_1 = 45, \varphi_2 = 60, \varphi_3 = 85, \varphi_4 = 65, \varphi_5 = 130, \varphi_6 = 115, \varphi_7 = 160\}$. Na qual todos os atrasos estão indicados em picossegundos e as fases em grau.

5.1 Diagramas de constelações

A Fig. 23 apresenta os diagramas de constelações referentes aos sinais (a) gerado pelo transmissor, (b) codificado e (c) decodificado. Observando a Fig. 23 (a), percebe-se que o diagrama de constelação do sinal gerado pelo transmissor não apresenta distorções em seus pontos e estes estão distribuídos adequadamente. Isto ocorre, uma vez que este representa um sinal sem degradação e conseqüentemente livre de erros de bits ($BER_D < 10^{-15}$).

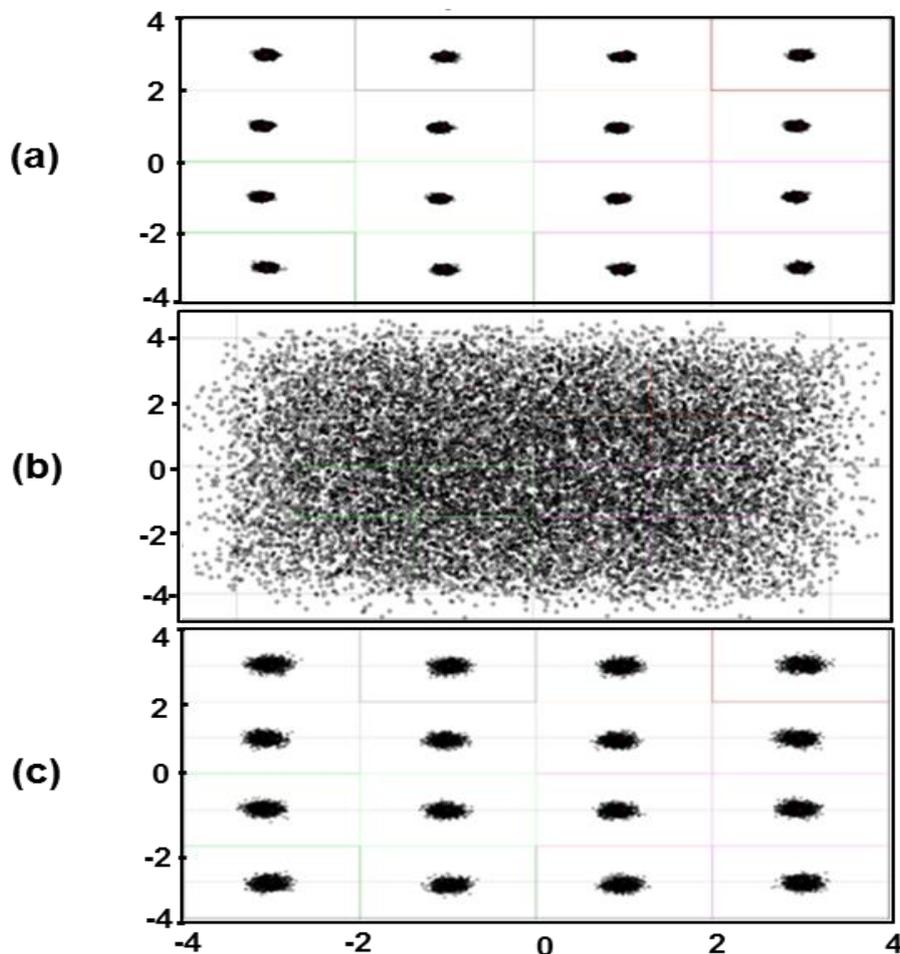


Figura 23 - Diagramas de constelações referentes aos sinais, (a) gerado pelo transmissor, (b) codificado e (c) decodificado

Ainda na Fig. 23, observar-se um comportamento relativamente análogo ao observado em resultados de simulações no domínio do tempo, apresentado

em seções anteriores. Naqueles resultados, foi possível observar o sinal codificado degradado por intermédio de suas representações. Isto é, representações das sequências de bits e diagramas de olho. Deste modo, observa-se também embaralhamento e distorções nos pontos de constelação do diagrama do sinal codificado, ilustrado na Fig. 23 (b). Estas distorções, tal como em casos anteriores, são causadas pela degradação artificial do sinal pela *COBFE*. Segundo resultados de simulações, BER_C referente a este diagrama é estimada em 35%.

Na Fig. 23 (c) observa-se que o diagrama de constelação do sinal decodificado apresenta pequenas distorções se comparado ao sinal gerado pelo transmissor. Porém, tais distorções não são suficientes para degradar o sinal. Consequentemente, os pontos de constelação do sinal decodificado estão distribuídos de maneira adequada e assemelham-se ao diagrama referente ao sinal gerado pelo transmissor. Resultados de simulações indicam que BER_D referente a este sinal é livre de erro de bits.

5.2 Análise dos espectros ópticos

A Fig. 24 apresenta os espectros ópticos dos sinais, (a) gerado pelo transmissor, (b) codificado e (c) decodificado. Diferente dos resultados referente ao diagrama de constelação apresentados na Fig. 23 (b), o espectro óptico do sinal codificado (Fig. 24 b) não apresenta distorções significantes que pudessem comprometer o desempenho da técnica. Este comportamento também foi observado em simulações com sinais modulados com *DPSK* e *DQPSK*.

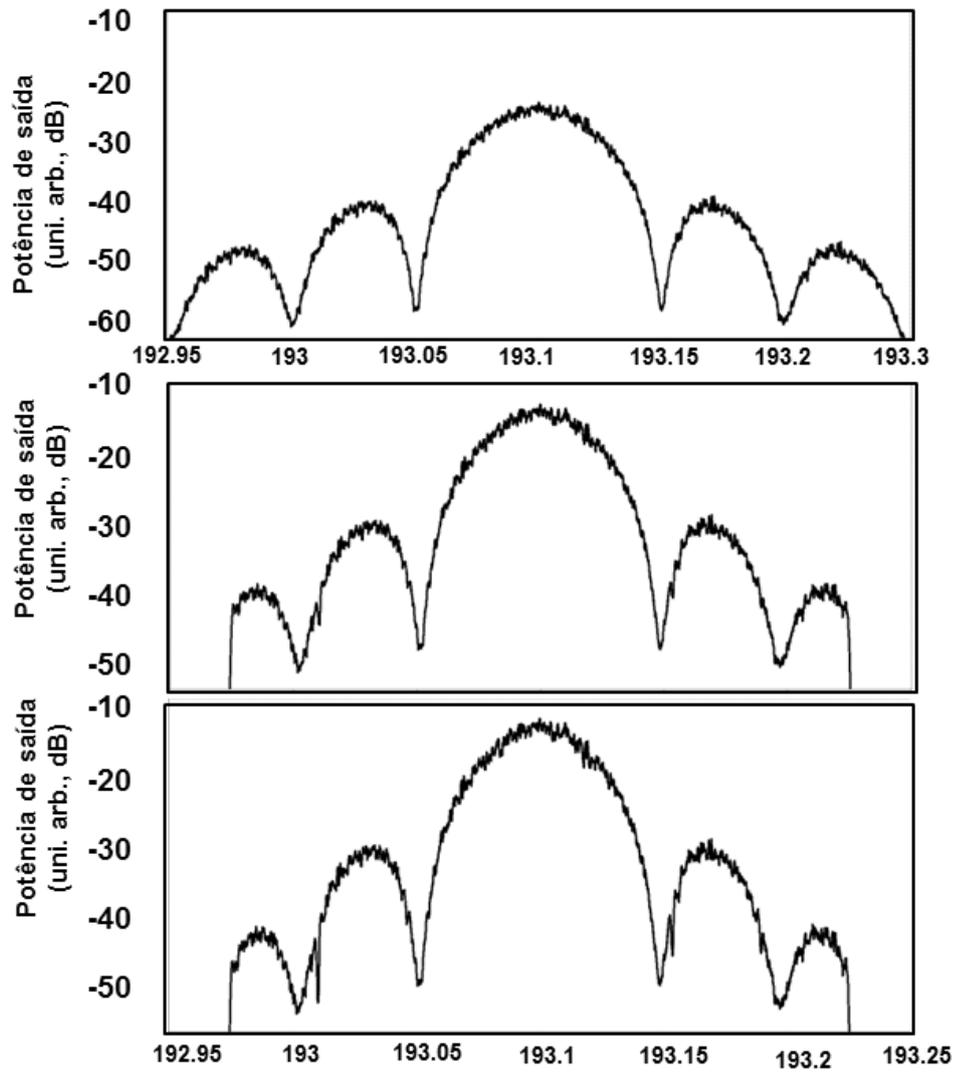


Figura 24 - Espectros ópticos dos sinais, (a) gerado pelo transmissor, (b) codificado e (c) decodificado.

5.3 Influência do atraso na taxa de erro de bits do sinal codificado em função da fatia espectral

Para efeito de avaliação da robustez da *COBFE*, foi realizado um estudo para avaliar a influência do atraso em BER_C em função da fatia espectral. Este estudo foi realizado adotando os mesmo critérios apresentados na Seção 3.2, porém, com o atraso variando de 5 a 50 ps. Uma vez que, para este formato de modulação a taxa estabelecida foi de 200 Gbps, confere um período de símbolo de 5 ps. Os resultados referentes a estes estudos são apresentados na Fig. 25.

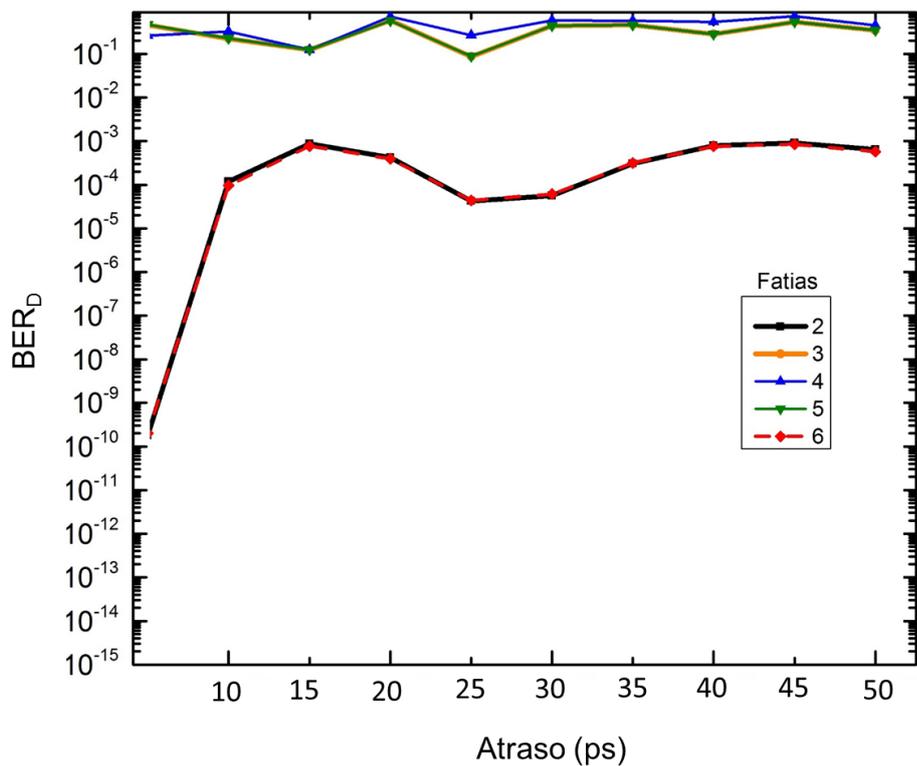


Figura 25 - Influência do atraso na taxa de erro de bits do sinal codificado em função da fatia espectral

De maneira geral, para qualquer formato de modulação, a energia mais significativa está localizada nas frequências centrais do espectro. Dessa forma, para o formato *16-QAM* o mesmo ocorre para nas fatias codificadas. Sendo assim, pode-se observar no gráfico que as curvas para variações de τ_3 , τ_4 e τ_5 , mostram que para a codificação em atraso apenas nas fatias centrais, (fatias 3, 4 e 5), BER_C varia de 10^{-2} a 10^{-1} , isso para o intervalo de 5 a 50 ps.

As curvas referentes às codificações das fatias 2 e 6 (τ_2 e τ_6), no intervalo de 10 a 50 ps, apresentam variações em BER_C de 10^{-5} a 10^{-4} . Entretanto, as curvas das demais fatias não foram apresentadas no gráfico por apresentarem BER_C inferiores a 10^{-15} . Isto faz sentido, uma vez que, estas fatias não contém parcela de energia significativa no espectro a ponto de afetar a codificação do sinal.

5.4 Influência da fase na taxa de erro de bits do sinal codificado em função da fatia espectral

A Fig. 26 ilustra as curvas referentes ao estudo realizado para análise da influência da taxa de erro de bits do sinal codificado em função da fatia espectral. Para realização destes estudos, foram adotados os mesmos critérios usados em simulações anteriores.

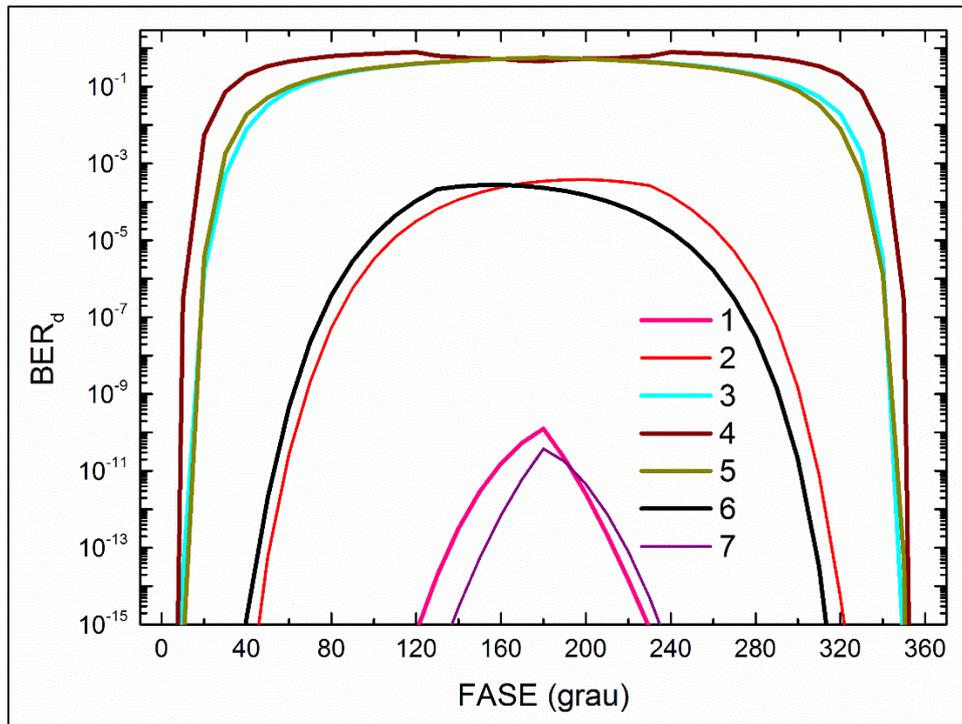


Figura 26 - Influência de φ_c em BER_c em função da fatia espectral.

Em gráficos de resultados anteriores (Figuras 8 e 12), observou-se que as curvas dos gráficos apresentaram simetrias em relação ao eixo vertical na posição de 180° no eixo X , isto é, $BER(\theta) = BER(-\theta)$. Na Fig. 26, é possível observar que tal comportamento se repete com a codificação em fase em sinais modulados com 16-QAM. No entanto, estes resultados sugerem que, para esta modulação, a utilização de codificação em fase com até 180° ou superior também é de caráter opcional.

Ainda na Fig. 26, observa-se também que, tal como as figuras ilustradas anteriormente (Figuras 19 e 25), as fatias espectrais com fases inferiores a 30° têm pouca influência na codificação. No entanto, a partir de 40° a 180° , BER_c para as fatias espectrais centrais, (fatias 3, 4 e 5), foi inferior a 10^{-3} .

Nessa mesma figura (Fig. 26), nota-se a presença das curvas referentes as 7 fatias espectrais. De fato, os resultados destas simulações sugerem que a codificação em fase para sinais modulados com 16-QAM apresenta melhor desempenho se comparada com resultados referentes a codificação em fase em sinais modulados com *DPSK* e *DQPSK*.

5.5 Influência do número e posição das fatias espectrais na taxa de erro de bits do sinal codificado em função da relação sinal-ruído óptica

Para avaliar a influência de BER_C em função da $OSNR$, foram realizadas diversas simulações e seus resultados são apresentados na Fig. 27. Todavia, vale realçar que nestes foram adotados os mesmos procedimentos usadas em estudos apresentados em seções anteriores (Seções 3.4 e 4.4).

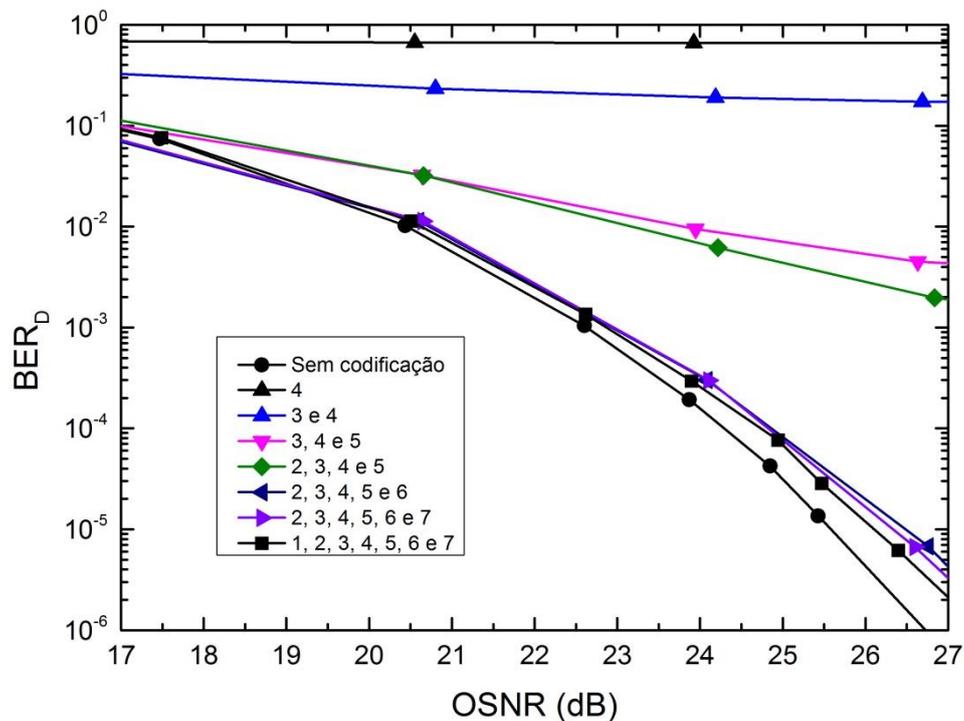


Figura 27 - Influência do número e posição das fatias espectrais na BER_C

A Fig. 27 sugere que, na codificação com a modulação 16-QAM, para que um intruso consiga recuperar o sinal, diferente dos casos anteriores, neste, o intruso precisa conhecer os parâmetros de 5 fatias para obter BER_D de 10^{-3} e uma $OSNR$ de 23 dB. Lembrando que, é possível recuperar sinal com BER nessa ordem de grandeza por intermédio de FEC .

Ainda na Fig. 27, observa-se também que, tal como concluído em seções anteriores, a modulação 16-QAM mostrou ser mais sensível à $COBFE$, uma vez que tanto na variação do atraso como no desvio de fase a codificação foi relativamente significativa em todas as fatias espectrais.

6. ANÁLISE DOS RESULTADOS DE SIMULAÇÕES MEDIANTE A UTILIZAÇÃO DE FILTRAGEM DIGITAL DE NYQUIST E FILTROS ÓPTICOS SUPERGAUSSIANOS DE 5 ORDEM

Neste capítulo são apresentados resultados da *COBFE* mediante a utilização de filtros supergaussianos de 5ª ordem e filtragem digital de *Nyquist* para sinais modulados com *16-QAM*. Na Seção 1 são mostrados os perfis dos filtros reais e ideais de cada fatia, bem como o fatiamento espectral do sinal. Em seguida, a Seção 2 discute os resultados de simulações *back-to-back*. Posteriormente, na Seção 3 serão mostrados resultados de propagação em rede. Os resultados de simulações com codificação em 14 fatias serão apresentados na Seção 4. Finalizando o capítulo, na Seção 5 serão apresentados e discutidos os resultados de simulações com duas codificações em sinais propagados.

Nas simulações referentes aos resultados representados nesta seção, foi utilizada a filtragem digital de *Nyquist*. Essa filtragem é mais eficiente por ser feita no domínio digital e não no domínio óptico, como é o caso de filtros ópticos. Com a filtragem digital de *Nyquist* é possível filtrar o sinal de forma bem abrupta e deixando passar um nível de ruído muito reduzido se comparado com filtros ópticos convencionais que apresentam perfis gaussianos, o que insere mais ruído no sinal. Deste modo, é possível transmitir, por exemplo, um sinal *16-QAM* de 200 *Gbps* na grade do ITU de 50 *GHz*.

6.1. Fatiamento Espectral

A Fig. 1 apresenta o esquema das fatias (a) com filtros ideais de perfis retangulares e (b) com filtros supergaussianos de 5ª ordem. Observa-se que na Fig. 1 (a) com a utilização de filtros ideais, as fatias são adjacentes e não há sobreposição entre elas. Porém, na Fig. 1 (b) observa-se que mediante a utilização de filtros reais, há sobreposição das fatias que resulta em interferência entre os sinais dessas fatias, tanto no codificador como no decodificador. Conseqüentemente, a interferência dos sinais causada pela sobreposição das fatias interfere também no desempenho da *COBFE*. Sendo assim, estes resultados sugerem que, para a *COBFE*, quanto mais abrupto for o filtro utilizado, menor é a interferência entre sinais das fatias e melhor é o desempenho da técnica.

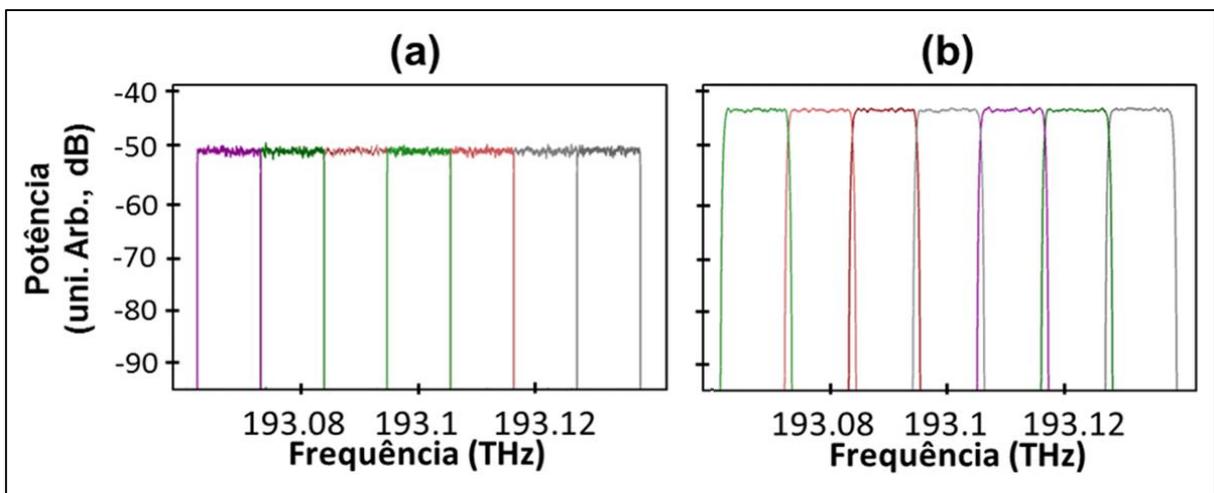


Figura 28 - Disposição dos filtros em frequência. (a) Filtros ideais com perfis retangulares, (b) Filtros reais supergaussianos de 5 ordem

A Fig. 2 apresenta os fatiamentos espectrais do sinal 16-QAM. Nesta figura é possível observar a sobreposição entre as fatias espectrais que resulta na interferência entre os sinais.

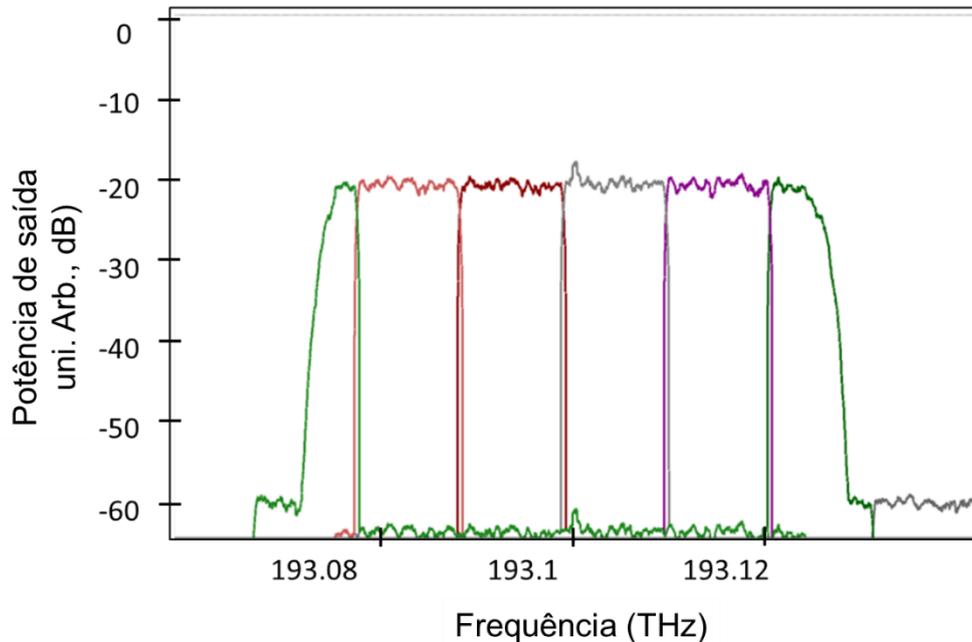


Figura 29 -Fatiamento espectral do sinal 16-QAM mediante a utilização de filtragem digital de Nyquist

6.2. Resultados de simulações de propagação em rede.

A Fig. 2 apresenta os resultados de simulações com os sinais propagados em rede de 350 km (a) gerado pelo transmissor, (b) codificado e (c) decodificado. Na Fig. 2 (a) nota-se o diagrama de constelação apresenta os pontos bem definidos, o que corresponde a um sinal sem degradação ou relativamente livre de erros. Na Fig. 2 (b) observa-se que o diagrama de constelação está completamente distorcido e os pontos estão espalhados, o que corresponde a um sinal degradado, tal como discutido em seções anteriores. Segundo

resultados de simulações, para uma $OSNR$ de 21,6 dB, BER_C foi estimada em 74%. No sinal após o decodificador, isso após 350 km, BER_D foi estimada em 10^{-4} . Tal como discutido em seções anteriores, essa BER_D pode ser melhorada com a utilização de FEC.

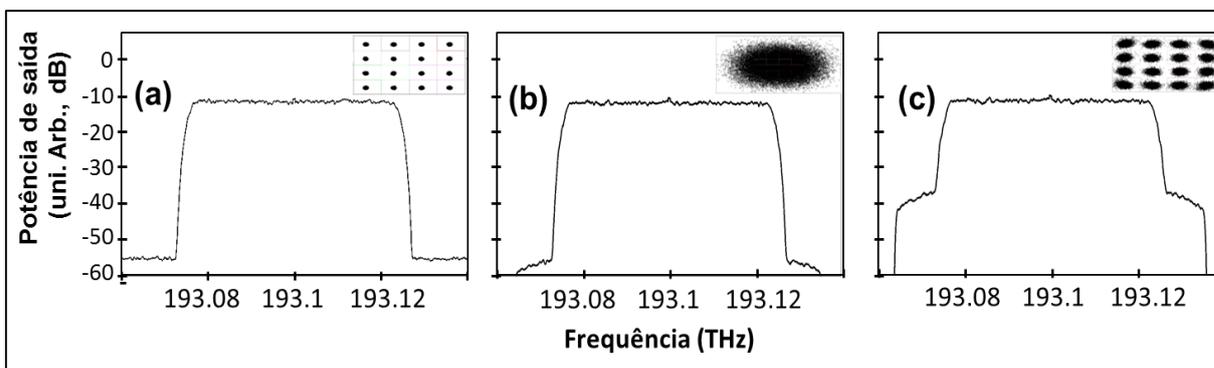


Figura 30 - Resultados de simulações com sinais 16-QAM em 350 km.

6.3. Resultados de simulação de propagação em rede com sinal codificado com em 14 fatias

Quanto maior for o número de fatias, mais robusta a técnica se torna. Para que se possa aumentar o número de fatias sem aumentar a banda é necessária que se tenha filtros com largura de banda mais estreita, que atualmente não são encontradas comercialmente. Nesse contexto, foram utilizados dois codificadores em série com sete fatias cada, porém em frequências diferentes para que totaliza 14 fatias sem a necessidade de alterar os filtros. Após este processo, o sinal foi propagado em 350 km para 16-QAM.

A Fig. 3 apresenta o esquemático usado para as simulações com duas codificações. Neste esquemático, **TX** corresponde ao Transmissor, **EDFA_c** ao

Amplificador que é usado para manter a potência em 1 mW, **C₁** e **C₂** correspondem aos Codificadores 1 e 2, **OBPF** é referente aos Filtros usados para redução do ruído após a codificação e decodificação dos sinais, **STDF** à Fibra padrão, **DCF** à Fibra de compensação de dispersão, **D₁** e **D₂** correspondem aos decodificadores e **Rx** é o Receptor do sinal.



Figura 31 – Esquemático das simulações com 14 fatias

Os dois codificadores, **C₁** e **C₂**, possuem seta fatias cada, estão no mesmo enlace e foram codificados com chaves diferentes. Todas as fatias de **C₂** foram deslocadas em 3 GHz com relação às fatias de **C₁**, o que totaliza 14 fatias.

A Fig. 4 apresenta os resultados de simulações do sinal codificado com 14 fatias (a) **C₁**, (b) **C₂**, (c) **D₂** e (d) **D₁**. Observa-se que os espectros estão apenas limitados por banda. Os diagramas de constelações referentes à **C₁**, **C₂** e **D₂** estão completamente distorcidos e apresentam pontos muito embaralhados. Para uma OSNR de 21,6 dB, BER referente aos estágios de **C₁**, **C₂** e **D₂** foi superior a 73% e para o estágio **D₁** foi de aproximadamente $1,1 \cdot 10^{-3}$, tal como detalha a Tabela 3.

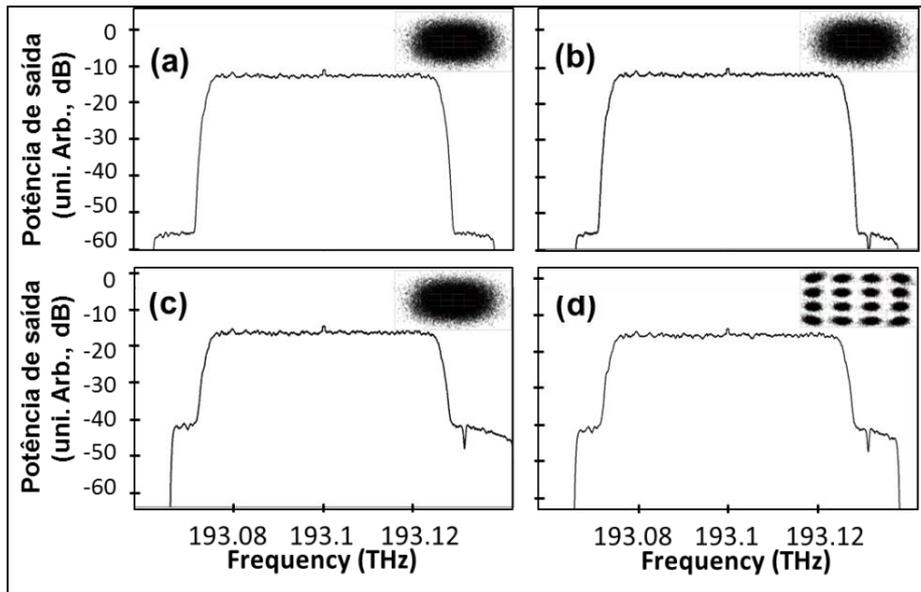


Figura 32 - Resultados de simulação com 14 fatias para sinais 16-QAM em 350 km.
 (a) Sinal no codificador 1, (b) Sinal no codificador 2, (c) Sinal no decodificador 2
 (b) e (c) Sinal no decodificador 1

Tabela 2 - Resultada de simulações da COBFE com 14 fatias

16-QAM codificação em 14 fatias	
ESTÁGIO	BER
BER _{C1}	74%
BER _{C2}	82%
BER _{D2}	75%
BER _{D1}	1.10^{-3}
OSNR	21.6

6.4. Resultados de simulação com duas codificações

Outro estudo realizado foi para avaliar a COBFE em casos que se precisa codificar o sinal mais de uma vez. Nesse estudo é suposto que uma operadora

de telecomunicações, O_1 , solicite serviços para uma segunda operadora, O_2 . A O_2 obviamente sem saber que O_1 já havia codificado o sinal, ela codifica novamente com uma chave diferente. Desse modo, o sinal é codificado duas vezes e conseqüentemente precisa ser decodificado duas vezes também.

A Fig. 3 mostra o esquemático usado para as simulações com duas codificações. Diferente do esquemático apresentado anteriormente (Fig.3), Na Fig. 5, C_1 e C_2 representam os codificadores das operadoras, O_1 e O_2 . D_1 e D_2 correspondem aos decodificadores das mesmas operadoras (O_1 e O_2).

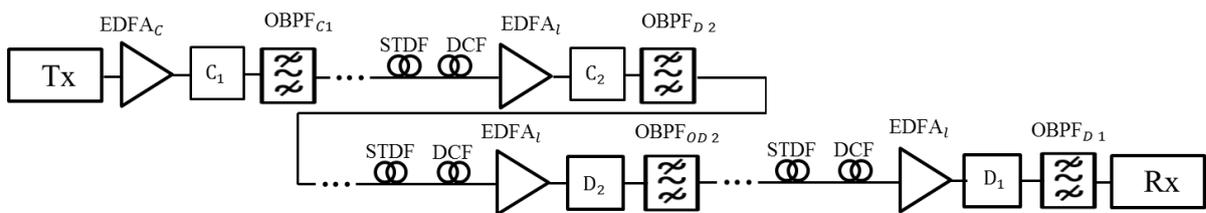


Figura 33 – Esquemático das simulações com duas codificações

A Fig. 5 apresenta os resultados de simulações do sinal propagado com duas codificações (a) C_1 , (b) C_2 , (c) e (d) D_2 . Nesta figura, observa-se que os espectros dos sinais também estão limitados em banda. Os pontos de constelação dos diagramas nas Figs. (a), (b) e (c) estão totalmente distorcidos e embaralhados, uma vez que, BER associada a esses sinais é superior a 73%.

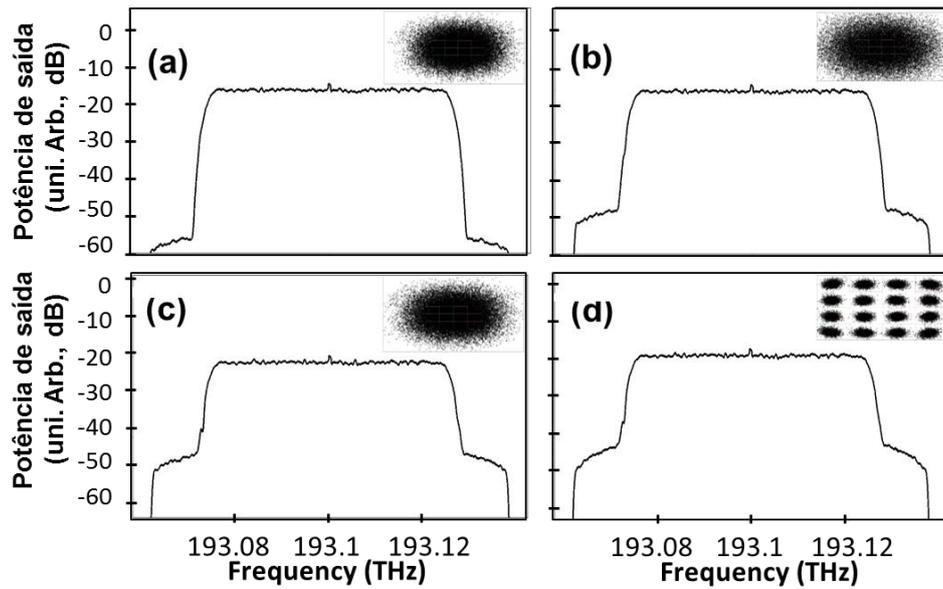


Figura 34 - Resultados de simulação com 2 codificações para sinais 16-QAM em 350 km (a) Sinal no codificador 1, (b) Sinal no codificador 2, (c) Sinal no decodificador 2 (a) e (c) Sinal no decodificador 1

A Tabela 3 apresenta os resultados referentes a essas simulações. De facto, o sinal só é recuperado no D_1 , uma vez que, seriam necessárias as duas chaves de decodificação para recuperar o sinal. Resultados de simulações indicam que, para uma OSNR de 21,6 dB, BER_D é estimada em $7,4 \cdot 10^{-4}$.

Tabela 3 - Resultado de simulações da COBFE com duas codificações

16-QAM com duas codificações	
ESTÁGIO	BER
BER_{C1}	74%
BER_{C2}	82%
BER_{D2}	75%
BER_{D1}	$7.4 \cdot 10^{-4}$
OSNR	21.6

6.5. Influência do número e posição das fatias espectrais na taxa de erro de bits do sinal decodificado em função da relação sinal-ruído óptica

A Fig. 8 mostra a influência das fatias espectrais em BER_D em função da $OSNR$ mediante a utilização de filtragem digital de *Nyquist*. Observa-se que, acertando quatro fatias espectrais centrais, BER_D ainda se mantém em 10^{-1} , para que um intruso consiga BER de aproximadamente 10^{-3} , precisaria conhecer parâmetros de 5 fatias com $OSNR$ de 21 dB. Caso a $OSNR$ fosse inferior a 19 dB, o intruso precisaria conhecer os parâmetros de exatamente todas as fatias.

Tal como mencionado anteriormente, a filtragem digital de *Nyquist* deixa o espectro mas plano e abrupto. Consequentemente, há maior distribuição de energia entre as fatias. Essa característica dos filtros de *Nyquist* influencia positivamente no desempenho da *COBFE*, fazendo com que a codificação nas fatias laterais seja mais significativa.

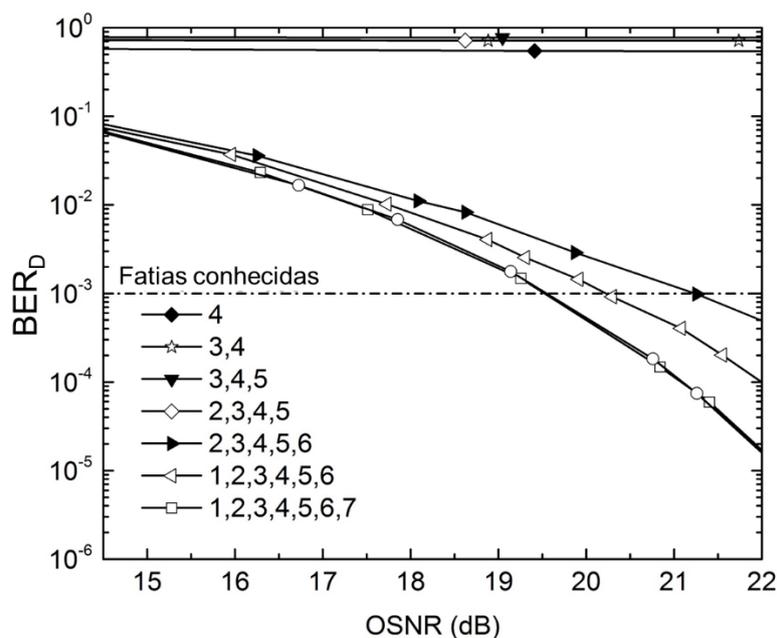


Figura 35 – Influência do número e posição da fatia espectral em BER_D em função da $OSNR$

7. CONCLUSÃO

A técnica de criptografia do sinal óptico avaliada neste trabalho foi inicialmente proposta em [28]. Nessa proposta, o sinal era dividido em diversas fatias espectrais e a codificação era realizada por intermédio da variação da atenuação e atraso dos bits de cada uma dessas fatias.

Segundo resultados de trabalhos anteriores [28], a codificação por intermédio da variação do atraso nas fatias espectrais não era suficientemente segura, uma vez que, por meio de análises espectrais seria possível identificar quais componentes do espectro haviam sido alteradas. Deste modo, ficaria relativamente fácil um intruso provido de alguns equipamentos e conhecimento na área recuperar as informações do sinal com a compensação das atenuações inseridas nas fatias.

Neste contexto, a técnica de criptografia anteriormente proposta, foi avaliada neste trabalho para dois estágios de codificação do sinal óptico. No primeiro estágio, após o sinal ser sido dividido em diversas fatias espectrais, é aplicada então a codificação baseada em fase. No segundo, as fatias espectrais são submetidas a diferentes atrasos de bits/símbolos. Um dos grandes desafios foi encontrar *OBPFs* disponíveis na literatura que fossem compatíveis com a *COBFE*. Isto finalmente foi possível por intermédio da sobreposição de um filtro de fotônica de silício disponíveis na literatura [36].

Nos Capítulos 3, 4 e 5 foram apresentados resultados de simulações da *COBFE* para os sinais modulados com *DPSK*, *DQPSK* e *16-QAM*, com taxas de

transmissão de 40 Gbps para sinais *DPSK* e *DQPSK*, e 200 Gbps para sinal 16-QAM. Para os três formatos de modulações, os sinais foram analisados nos domínios do tempo e frequência. No domínio do tempo, foram avaliadas as representações das sequências de bits e diagramas de olho. Tal como esperado, os bits do sinal codificados estavam relativamente embaralhados e distorcidos, e em todos os casos, BER_C foi superior a 10% - limiar mínimo estabelecida neste trabalho para a codificação. Nos diagramas de olho e constelação dos sinais codificados, também foi possível observar distorções que os tornassem ilegíveis. De fato, isso faz sentido, uma vez que a codificação é realizada por intermédio da degradação artificial do sinal pela *COBFE*. Tanto as representações das sequências de bits como os diagramas de olho e constelação dos sinais dos três sinais decodificados se assemelharam às respectivas representações dos sinais gerados pelo transmissor.

Nos espectros dos sinais codificados referentes aos formatos de modulações *DPSK*, *DQPSK* e 16-QAM, as alterações são mínimas e não são suficientes para identificar as referidas codificações. Nestes espectros, um intruso ou qualquer pessoa não autorizada teria dificuldades em identificar a codificação utilizada, uma vez que este espectro também se assemelha ao gerado pelo transmissor. Resultados de simulações referentes ao sinal decodificado indicaram BER_D para os três formatos de modulação é inferior a 10⁻¹⁵.

Estes resultados corroboram com os apresentados em [28], que sugere que a *COBFE* é transparente ao tipo de modulação, uma vez que, a *COBFE* mostrou-se eficaz para todos os formatos de modulações testados.

Observou-se também que, tanto a codificação em atraso como em fase podem ser implementadas de modo individual. Porém, a utilização simultânea dos dois módulos de codificação torna a técnica mais robusta. Outro ponto interessante a considerar, reside no fato de que a codificação em fase com valores superiores a 180 graus pode ser de caráter opcional. Isso deve a simetria entre os ângulos na posição 180 graus.

Em resultados sobre a influência da *OSNR* em BER_C em função da fatia espectral, observou-se que para a codificação em todas fatias e para os três formatos de modulações, a *OSNR* foi superior a 20 dB. De fato, durante uma propagação, a *OSNR* piora de acordo com o número de amplificadores e a distância. Em outras simulações da *COBFE* observou-se que com *OSNR* acima de 20 dB é possível propagar por distâncias superiores a 400 km com BER_D inferior a 10^{-15} .

Em resultados apresentados no Capítulo 6, observou-se que a filtragem digital de *Nyquist* melhora o desempenho da *COBFE*, fazendo com que haja maior distribuição de energia nas fatias espectral e, conseqüentemente, a codificação tem influência em um número maior de fatias espectrais.

Ainda no Capítulo 6, foram apresentados estudos do sinal codificado com 14 fatias e propagado em 350 km. Segundo resultados de simulações, com a codificação em 14 fatias, BER_C teve um aumento de aproximadamente 10% e BER_D foi de aproximadamente $1,1 \cdot 10^{-3}$, que pode ser melhorada mediante a utilização de *FEC*.

Outra avaliação apresentada no Capítulo 6, foi para avaliar a *COBFE* em situações em que se precisa codificar o sinal mais de uma vez. Nessa avaliação,

tal como esperado, o sinal só foi recuperado somente após o último estágio de decodificações. Esses resultados sugerem que a técnica é aplicável também em situações que o sinal precisa ser codificado e decodificado por diferentes operadoras de telecomunicações.

Em trabalhos anteriores [28-30], foram apresentadas simulações da *COBFE* para propagação de até 400 km com sinais modulados com *DPSK* e *DQPSK*, ambos com a taxa de transmissão de 40 *Gbps*. Em [30], foram mostrados os resultados para propagação de 16-QAM, isso também para taxa de transmissão de 200 *Gbps*. Para os três formatos de modulações foram possíveis atingir 400 km com BER_D inferiores a 10^{-3} sem a utilização da *FEC*. As distâncias utilizadas são aplicáveis em redes metropolitanas, o que viabilizaria sua utilização para este efeito.

Outro estudo foi realizado sobre a aplicação da *COBFE* com filtros ideais em redes *WDM* [26]. Neste mesmo estudo, concluiu-se que o sistema *WDM* apresenta baixo impacto no desempenho de BER_C , isso para simulações com até 15 canais a uma taxa de transmissão de até 100 *Gbps*. Nestas simulações, a *COBFE* mostrou ser eficiente em todos os canais com uma distância de 240 *km* sem *FEC*.

Com base em resultados satisfatórios obtidos neste e trabalhos anteriores para diferentes tipos de modulações e taxas de transmissões, pode-se dizer que a *COBFE* é transparente ao formato de modulação e taxa de transmissão. Além destes, a técnica é compatível com redes metropolitanas e *WDM*.

Como trabalhos futuros, seria importante estudar os comportamentos das chaves criptográficas e/ou desenvolver um algoritmo que pudesse gerá-las de

maneira automática, visto que, resultados de outros trabalhos indicaram que diferentes chaves não apresentam o mesmo desempenho. A técnica também poderia ser avaliada em diferentes tipos de filtros e/ou avaliar em filtros de fôtonica de silício. Outro estudo importante seria efetuar a codificação do sinal por intermédio do embaralhamento das fatias espectrais de diferentes canais. A técnica de codificação do sinal óptico por intermédio da polarização dos canais também pode ser avariada para codificar o sinal. Por exemplo, o sinal de 100 *Gbps* são dois sinais de 50 *Gbps*, um em cada polarização. Seria interessante testar a técnica de criptografia para os dois canais.

TRABALHOS PUBLICADOS

Marcelo L. F. Abbade, Member, IEEE, Carlos A. Messani, Cleiton J. Alves, Guilherme M. Taniguti, Iguatemi E. Fonseca, Eric A. M. Fagotto, Member, IEEE. A New All-Optical Cryptography Technique Applied to WDM-Compatible DPSK Signals. ICTON, 2013.

Carlos A. Messani,; Guilherme M. Taniguti; Cleiton J. Alves; Eric A. M. Fagotto; Marcelo L. F. Abbade; Iguatemi E. Fonseca. Transmission of Encrypted Optical Signals in a metropolitan WDM-compatible TON with Differential Phase-shift Keying Modulation. IMOC, 2013

M. L. F. Abbade , L. A. Fossaluzza Jr., C. A. Messani, G. M. Taniguti, E. A. M. Fagotto. All -Optical Cryptography through Spectral Amplitude and Delay Encoding Amplitude and Delay Encoding. JMOe. 2014.

Claudinei Martins; Carlos A. Messani; Cleiton J. Alves; Fagotto; Marcelo L. F. Abbade. All-Optical Narrowband Spectral Slicing Encryption with Supergaussian Filter. ITS. 2014

TRABALHOS SUBMETRIDOS

Marcelo L. F. Abbade, Gustavo H. Assis, Cleiton J. Alves, Carlos A. Messani, Eric A. M. Fagotto, Milorad Cvijetic. All-Optical Phase and Delay Spectral Encoding of Signals with Advanced Modulation Formats. ICTON, 2014.

8. REFERÊNCIAS

- [1] Sanou, Brahima. União Internacional de Telecomunicações, " ICTFACTS And Figures ". The World In 2014.
- [2] LCA Consultores, Confidencial, "Diagnóstico, cenários e ações para o Setor de Telecomunicações no Brasil, 2014 - 2020", Julho de 2011.
- [3] BRASSCOM, "Mapa de conectividade", Setembro de 2013.
- [4] Huawei Technologies CO., LTDA, " Balanço Huawei da Banda Larga 2T12", 2 trimestre de 2012.
- [5] Monteiro T. R., " A viabilidade futura do modelo de negócio da internet ", 56º Painel Telebrasil - 2012
- [6] Enéas G., Silva V., "Redes de Acesso Óptico para Próxima Geração Next Generation Optical Access Networks", Caderno de Estudos Ciência e Empresa, n. 2, nov. 2011.
- [7] Ministério da comunicacao, Anatel, CPqD, Telebrasil, " Um Plano Nacional para Banda Larga O Brasil em Alta Velocidade", 2012.
- [8] IPEA, "Desafios e Oportunidades do Setor de Telecomunicações No Brasil", Março de 2010.
- [9] Melo P. R. S, Gorin A. P. F., Rosa S. E. S., "Segmento de fios e cabos telefônicos: O Que Muda a partir da Fibra Óptica ?", Setembro, 2013.
- [10] Kaius Nevaste, "Optical Network Security", Department of Computer Science, Helsinki University of Technology, 1999.
- [11] <http://www.egerate.com/TM/Altesys/Aksesuarlar.htm>.

- [12] Mable P. Fok, Zhexing Wang, Yanhua Deng, Paul R. Prucnal, Fellow, "Optical Layer Security in Fiber-Optic Networks", IEEE Transactions On Information Forensics And Security, Vol. 6, NO. 3, September 2011.
- [13] Ken-Ichi Kitayama, Masahide Sasaki, Soichiro Araki, Makoto Tsubokawa, Akihisa Tomita, Kyo Inoue, Katsuyoshi Harasawa, Yuki Nagasako, Atsushi Takada, "Security in Photonic Networks: Threats and Security Enhancement", Journal Of Lightwave Technology, Vol. 29, NO. 21, November 1, 2011.
- [14] Augusto Marcacini, "Direito e Informática: uma abordagem jurídica sobre a criptografia", Editora eletrônica, Pags. 19- 37, sao paulo 2010.
- [16] Pedro A. D. Rezende, "Criptografia e Segurança na Informática", Departamento de Ciência da Computação, Universidade de Brasília.
- [17] Apostolos Argyris, Dimitris Syvridis, Laurent Larger, Valerio Annovazzi-Lodi, Pere Colet, Ingo Fischer, Jordi Garcí'a-Ojalvo, Claudio R. Mirasso, Luis Pesquera & K. Alan Shore, "Chaos-based communications at high bit rates using commercial fibre-optic links", NATURE, Vol 438, 17 November 2005.
- [18] Adrian Jacobo, Miguel C. Soriano, Claudio R. Mirasso, and Pere Colet, "Chaos-Based Optical Communications: Encryption versus Nonlinear Filtering", IEEE Journal of Quantum Electronics, VOL. 46, NO. 4, APRIL 2010.
- [19] Paul D. T., "Quantum cryptography on optical fiber networks", BT Laboratories, B55-13 1 D, Martlesham heath, Ipswich, 1P5 3RE, U.K.
- [20] Kartalopoulos S. V., "Quantum Cryptography For Secure Optical Networks", The University of Oklahoma.

- [21] Joaquin A. Cornejo, Carlos E. Perez, and Jean-Louis de Bougrenet de la Tocnaye, " WDM-Compatible Channel Scrambling for Secure High-Data-Rate Optical Transmissions", Journal Of Lightwave Technology, Vol. 25, NO. 8, AUGUST 2007.
- [22] Surinder Singh, Lovkesh, Xiaohua Ye, and R. S. Kaler, "Design of Ultrafast Encryption and Decryption Circuits for Secured Optical Networks", IEEE Journal of Quantum Electronics, VOL. 48, No. 12, December 2012.
- [23] Jean-Pierre Goedgebuer, Pascal Levy, Laurent Larger, Chii-Chang Chen, and William T. Rhodes, "Optical Communication With Synchronized Hyperchaos Generated Electrooptically", Ieee Journal Of Quantum Electronics, Vol. 38, NO. 9, September 2002.
- [24] Nobuyuki Kataoka, Member, Naoya Wada, Member, Xu Wang, Senior Member, Gabriella Cincotti, Senior Member, and Ken-ichi Kitayama, Fellow, "10Gbps-Class, Bandwidth-Symmetric, OCDM-PON System using Hybrid Multi-port and SSFBG En/Decoder".
- [25] Kousik Mukherjee," A method of implementation of frequency encoded all optical encryption decryption using four wave mixing", Optik 122 (2011) 1407– 1411.
- [26] L.-C. Yang, C.-C. Huang, S.-C. Yang, S.-L. Tsao, " Analysis of dynamic encoder and decoder for optical code-division-multiple-access networks", IET Optoelectronics, May 2009.
- [27] Katsuyoshi Harasawa, Osamu Hirota, Member, Kiichi Yamashita, Member, Makoto Honda, Kenichi Ohhata, Member, Shigeto Akutsu, Takeshi Hosoi, and Yoshifumi Doi, Quantum Encryption Communication Over a 192-km 2.5-Gbit/s Line With Optical Transceivers Employing Yuen-

2000 Protocol Based on Intensity Modulation ", Journal Of Lightwave Technology, Vol. 29, No. 3, February 1, 2011.

- [28] M. L. F. Abbade , L. A. Fossaluzza Jr, Rodrigo Frandsen da Silva e E. A. M. Fagotto, " Criptografia Óptica Mediante Controle Analógico da Amplitude e do Atraso de Fatias Espectrais: Análise para Sinais NRZ", MOMAG, Jao pessoa, 2012.

- [29] M. L. F. Abbade , L. A. Fossaluzza Jr., C. A. Messani, G. M. Taniguti, E. A. M. Fagotto, " All -Optical Cryptography through Spectral Amplitude and Delay Encoding", Journal of Microwaves, Optoelectronics and Electromagnetic Applications, Vol. 12, No. 2, December 2013 .

- [30] L. A. Fossaluzza Jr, " Criptografia óptica mediante o controle analogico da amplitude e do atraso das fatias espectrais: Analise para sinais NRZ e DQPSK", Dissertacao de mestrado, 2012.

- [31] R. F. Silva , "Analise da Criptografia óptica mediante o controle analogico da amplitude e do atraso das fatias espectrais gerada com perfis de filtros ópticos comerciais", Dissertacao de mestrado, 2012.

- [32] Marcelo L. F. Abbade, Carlos A. Messani, Cleiton J. Alves, Guilherme M. Taniguti, " A New All-Optical Cryptography Technique Applied to WDM-Compatible DPSK Signals", ICTON 2013.

- [33] Carlos A. Messani, Guilherme M. Taniguti, Cleiton J. Alves, Eric A. M. Fagotto, and Marcelo L. F. Abbade, Iguatemi E. Fonseca, "Transmission of Encrypted Optical Signals in a metropolitan WDM-compatible TON with Differential Phase-shift Keying Modulation", IMOC 2013.

- [34] Marcelo L. F. Abbade, Gustavo H. Assis, Cleiton J. Alves, Carlos A. Messani, Eric A. M. Fagotto, Milorad Cvijetic, " All-Optical Phase and Delay

Spectral Encoding of Signals with Advanced Modulation Formats", ICTON 2014.

- [35] Claudinei Martins, Carlos A. Messani, Cleiton J. Alves ,Fagotto and Marcelo L. F. Abbade, " All-Optical Narrowband Spectral Slicing Encryption with Supergaussian Filter". ITS, 2014
- [36] A. Anjali , T. Paul , M. Ronald Menendez, Shahab Etemad, Member, Janet Jackel, Senior Member, Jeffrey Young, Thomas Banwell, Member, IEEE, B. E. Little, S. T. Chu, Wei Chen, Wenlu Chen, J. Hryniewicz, Member, F. Johnson, D. Gill, O. King, R. Davidson, K. Donovan, and Peter J. Delfyett, Fellow, " Fully Programmable Ring-Resonator-Based Integrated Photonic Circuit for Phase Coherent Applications",Journal Of Lightwave Technology, Vol. 24, NO. 1, January 2006