

UNIVERSIDADE ESTADUAL PAULISTA “JÚLIO DE MESQUITA FILHO”
CÂMPUS EXPERIMENTAL DE SÃO JOÃO DA BOA VISTA
BACHARELADO EM ENGENHARIA ELETRÔNICA E DE TELECOMUNICAÇÕES

PHILIPP FARNETANI FRIEDRICH

CRIPTOGRAFIA DE SINAIS ÓPTICOS POR EMBARALHAMENTO E
CODIFICAÇÃO ESPECTRAL DE ATRASO E FASE

SÃO JOÃO DA BOA VISTA
2020

PHILIPP FARNETANI FRIEDRICH

CRIPTOGRAFIA DE SINAIS ÓPTICOS POR EMBARALHAMENTO E
CODIFICAÇÃO ESPECTRAL DE ATRASO E FASE

Trabalho de Conclusão de Curso apresentado à
Universidade Estadual Paulista “Júlio de Mesquita
Filho” como requisito para obtenção de título de
Bacharel em Engenharia Eletrônica e de
Telecomunicações

Orientador: Prof. Dr. Marcelo Luís Francisco
Abbade

SÃO JOÃO DA BOA VISTA

2020

F911c Friedrich, Philipp Farnetani
Criptografia de sinais ópticos por embaralhamento e codificação
espectral de atraso e fase / Philipp Farnetani Friedrich. -- São João da
Boa Vista, 2020
47 p. : il., tabs.

Trabalho de conclusão de curso (Bacharelado - Engenharia de
Telecomunicações) - Universidade Estadual Paulista (Unesp), Câmpus
Experimental de São João da Boa Vista, São João da Boa Vista
Orientadora: Marcelo Luís Francisco Abbade

1. Comunicações ópticas. 2. Criptografia. 3. Segurança de sistemas.
I. Título.

Sistema de geração automática de fichas catalográficas da Unesp. Biblioteca do Câmpus
Experimental de São João da Boa Vista. Dados fornecidos pelo autor(a).

Essa ficha não pode ser modificada.

UNIVERSIDADE ESTADUAL PAULISTA
“JÚLIO DE MESQUITA FILHO”
CÂMPUS EXPERIMENTAL DE SÃO JOÃO DA BOA VISTA
GRADUAÇÃO EM ENGENHARIA ELETRÔNICA E DE TELECOMUNICAÇÕES

TRABALHO DE CONCLUSÃO DE CURSO

CRİPTOGRAFIA DE SINAIS ÓPTICOS POR EMBARALHAMENTO E CODIFICAÇÃO
ESPECTRAL DE ATRASO E DE FASE

Aluno: Philipp Farnetani Friedrich

Orientador: Prof. Dr. Marcelo Luís Francisco Abbade

Banca Examinadora:

- Marcelo Luís Francisco Abbade (Orientador)
- André Alves Ferreira (Examinador)
- Cintya Wink de Oliveira Benedito (Examinadora)

A ata da defesa com as respectivas assinaturas dos membros encontra-se no
prontuário do aluno (Expediente nº 42/2018)

Dedico inteiramente este trabalho à minha mãe, uma mulher incrível e batalhadora, que me trouxe sozinha até este momento tão importante na minha vida.

AGRADECIMENTOS

Ao meu orientador, Prof. Dr. Marcelo Luís Francisco Abbade, pela sua dedicação e muita paciência durante todo o desenvolvimento deste trabalho.

Ao meu colega e amigo pessoal, Leonardo Diogo Bueno Bobadilla, por toda a ajuda e apoio durante a realização das simulações deste trabalho.

À Universidade Estadual Paulista Júlio de Mesquita Filho, por me acolher durante todos os meus anos de graduação

À minha família, em especial minha mãe e irmãos, por todo o apoio e auxílio que precisei para percorrer este caminho até hoje, e não ter me deixado desistir nunca.

Por fim, gostaria de agradecer a todos que fizeram parte da minha vida durante esses anos como aluno de graduação da Unesp. Não poderia ser mais grato por ter conhecido a todos.

“Foco, força e fé”

- José Tiago Sabino Pereira

RESUMO

O intenso aumento do tráfego de rede observado, desde a década de 1990, estimulou o desenvolvimento de tecnologias para ampliar a capacidade de transmissão de dados na Internet. Ao mesmo tempo que essa evolução popularizou o uso de computadores e de outros dispositivos de comunicações digitais, surgiram problemas relacionados à segurança de redes. Boa parte desses problemas é resolvida pela utilização de criptografia de dados. No entanto, os sinais que trafegam pelos enlaces das redes estão sujeitos à espionagem e, também, precisam ser protegidos. Para realizar essa tarefa, tem-se considerado o uso de criptografia de sinais. Em particular, as redes ópticas transparentes são atrativas para esse fim porque elas transmitem sinais da origem ao destino sem precisar processá-los. Portanto, para os nós de comutação deste tipo de rede, é indiferente se os sinais estão ou não criptografados. Além disso, as comunicações ópticas são responsáveis por transmitir a maior parte dos dados que passa pelo núcleo da rede de telecomunicações. Neste trabalho, é apresentada uma técnica de criptografia óptica, em que dois sinais ópticos distintos são submetidos a três estágios de criptografia. No primeiro, dois ou mais sinais são divididos em diversas fatias espectrais e as fatias desses sinais são embaralhadas entre si. No segundo estágio, cada fatia recebe um desvio de fase. No último estágio, as fatias são submetidas a atrasos da ordem de período de símbolos. Essa técnica é avaliada por meio de simulações no *software VPI Transmission Maker™ Optical Systems* (VPI) para sinais modulados por chaveamento de fase em quadratura (em inglês *quadrature phase shift keying*, QPSK) de 56 Gb/s. Os resultados sugerem que a razão de erro de bits (*bit error ratio*, BER) do sinal criptografado é de aproximadamente 0,5, dificultando a espionagem. Por outro lado, os sinais descriptografados podem ser recuperados com uma penalidade de 4 dB. Em termos de segurança, estima-se que sejam necessárias $2,164 \cdot 10^{103}$ tentativas para garantir o sucesso de ataques de força bruta.

Palavras-chave: Criptografia óptica, Comunicações ópticas, Segurança.

ABSTRACT

The intense increase in network traffic observed since the 1990s has stimulated the development of technologies to expand the data transmission capacity on the Internet. At the same time that this evolution popularized the use of computers and other digital communications devices, problems related to network security arose. Much of these problems are solved by using data encryption. However, the signals that travel through the network links are subject to espionage and also need to be protected. To accomplish this task, the use of signal encryption has been considered. In particular, transparent optical networks are attractive for this purpose because they transmit signals from source to destination without having to process them. Therefore, for switching nodes of this type of network, it does not matter whether the signals are encrypted or not. In addition, optical communications are responsible for transmitting most of the data that passes through the core of the telecommunications network. In this work, an optical encryption technique is presented, in which two distinct optical signals are submitted to three stages of encryption. In the first, two or more signals are divided into several spectral slices and the slices of these signals are shuffled together. In the second stage, each slice receives a phase shift. In the last stage, the slices are subjected to delay of the symbol period order. This technique is evaluated through simulations in the VPI Transmission Maker [™] Optical Systems (VPI) software for signals modulated by quadrature phase shift keying (QPSK) of 56 Gb/s. The results suggest that the bit error ratio (BER) of the encrypted signal is approximately 0.5, making espionage difficult. On the other hand, the decrypted signals can be recovered with a penalty of 4 dB. In terms of security, it is estimated that $2,164 \cdot 10^{103}$ attempts are required to ensure the success of brute force attacks.

Keywords: *Cryptography, Optical communications, Security.*

LISTA DE FIGURAS

Figura 1 – Brasileiros com acesso à Internet entre os anos de 2000 e 2017	1
Figura 2 – Janelas das comunicações ópticas	2
Figura 3 – Amplificadores, multiplexador e demultiplexador óptico	5
Figura 4 – Arranjo divisor de fatias (em inglês spectral slicer setup, SSS), operando com SLM em modo de amplitude	12
Figura 5 – Arranjo deslocador de fase (em inglês phase shifter setup, PSS), operando com o SLM em modo de fase	13
Figura 6 – Arranjo gerador de atraso (em inglês delay maker setup, DMS), operando com um arranjo de espelhos	14
Figura 7 – Processo de encriptação do sinal óptico	15
Figura 8 – Processo de desencriptação de um sinal óptico	17
Figura 9 – Diagrama de blocos do canal óptico do arranjo	20
Figura 10 – Detecção Coerente Homódina, com utilização de Processamento Digital de Sinais	23
Figura 11 – Gráfico da BER em função da OSNR para um canal AWGN B2B, sem uso da técnica de criptografia, 128, 256 e 330 fatias encriptadas	25
Figura 12 – Gráfico da BER em função da OSNR para um canal AWGN com 400 km de propagação, sem uso da técnica de criptografia e 330 fatias encriptadas	27
Figura 13 – Gráfico da BER em função da OSNR para um canal AWGN com 400 km de propagação, sem uso da técnica de criptografia e 330 fatias encriptadas, comparado à técnica AOSS	28

LISTA DE TABELAS

Tabela 1 – Relação de comprimento de onda com atenuação, nas janelas do domínio óptico	3
Tabela 2 – Comprimento de onda das bandas espectrais utilizadas em comunicações ópticas	3
Tabela 3 – Parâmetros dos elementos existentes na TON do arranjo	21
Tabela 4 – Comparação de OSNR mínima de recuperação	29
Tabela 5 – Penalidade confrontada de OSNR mínima de recuperação	29

LISTA DE SIGLAS E ABREVIATURAS

AES	<i>Advanced Encryption Standard</i>
AOSS	<i>All-Optical Encryption Using Multi-Channel Spectral Shuffling</i>
ASE	<i>Amplified Spontaneous Emission</i>
ASK	<i>Amplitude Shift Keying</i>
AWGN	<i>Additive White Gaussian Noise</i>
B2B	<i>Back-To-Back</i>
BC	<i>Beam Combiner</i>
BER	<i>Bit Error Rate</i>
bit	<i>Binary Digit</i>
BOA	<i>Booster Optical Amplifier</i>
BPSK	<i>Binary Phase Shift Keying</i>
BS	<i>Beam Splitter</i>
CSL	<i>Convergent Spherical Lens</i>
CWDM	<i>Coarse Wavelength Division Multiplexing</i>
DCF	<i>Dispersion Compensation Fiber</i>
DEMUX	Demultiplexador Óptico
DG	<i>Diffraction Grating</i>
DMS	<i>Delay Maker Setup</i>
DP-QPSK	<i>Dual-Polarization Quadrature Phase Shift Keying</i>
DSP	<i>Digital Signal Processing</i>
DWDM	<i>Dense Wavelength Division Multiplexing</i>
EDFA	<i>Erbium-Doped Fiber Amplifier</i>
FEC	<i>Forward Error Correction</i>
FWM	<i>Four Wave Mixing</i>
GCHQ	<i>Government Communications Headquarters</i>
ITU	<i>International Telecommunications Union</i>
LASER	<i>Light Amplification By Stimulated Emission Of Radiation</i>
LCD	<i>Liquid Crystal Display</i>
LO	<i>Local Oscillator</i>
LOA	<i>Line Optical Amplifier</i>
MUX	Multiplexador Óptico

NSA	<i>Nacional Security Agency</i>
OCDMA	<i>Optical Code Division Multiple Access</i>
OOK	<i>On-Off Keying</i>
OSI	<i>Open System For Interconnections</i>
OSNR	<i>Optical Signal-To-Noise Ratio</i>
POA	<i>Pre-Optical Amplifier</i>
PRBS	<i>Pseudorandom Bit Sequence</i>
PSK	<i>Phase Shift Keying</i>
PSS	<i>Phase Shifter Setup</i>
QPSK	<i>Quadrature Phase Shift Keying</i>
SLM	<i>Spatial Light Modulator</i>
SMF	<i>Single Mode Fiber</i>
SPDE	<i>Spectral Phase And Delay Encoding</i>
SPE	<i>Spectral Phase Encoding</i>
SSS	<i>Spectral Slicer Setup</i>
TON	<i>Tranparent Optical Networks</i>
VPI	<i>Software Vpi Transmission Maker™ Optical Systems</i>
WAN	<i>Wide Area Network</i>
WDM	<i>Wavelenght Division Multiplexing</i>
XOR	<i>OR Exclusive</i>
XPM	<i>Cross-Phase Modulation</i>
XPoLM	<i>Cross Polarization Modulation</i>

LISTA DE SÍMBOLOS

α_{SMF}	Atenuação da fibra monomodo.
$\Delta\theta$	Erro máximo que o invasor pode cometer para ainda acertar a fase da fatia espectral.
ϕ	Deslocamento de fase.
ϕ'	Deslocamento de fase complementar para 360°.
τ	Atraso aplicado à fatia espectral.
c	Velocidade da luz.
CSL_A	Lente Esférica Convergente do arranjo em 4F que utiliza-se de um SLM em modo de amplitude, arranjo divisor de fatias (em inglês <i>spectral slicer setup</i> , SSS).
CSL_ϕ	Lente Esférica Convergente do arranjo em 4F que utiliza-se de um SLM em modo de fase, arranjo deslocador de fase (em inglês <i>phase shifter setup</i> , PSS).
CSL_τ	Lente Esférica Convergente do arranjo em 4F do gerador de atraso (em inglês <i>delay maker setup</i> , DMS).
d	Distância específica entre os espelhos do arranjo de espelhos do arranjo gerador de atraso (em inglês <i>delay maker setup</i> , DMS).
D_{DCF}	Dispersão cromática das fibras compensadoras de dispersão.
$D(f)$	Sinal óptico descriptado na recepção.
DG_A	Grade de difração do arranjo em 4F que utiliza-se de um SLM em modo de amplitude, arranjo divisor de fatias (em inglês <i>spectral slicer setup</i> , SSS).
DG_ϕ	Grade de difração do arranjo em 4F que utiliza-se de um SLM em modo de fase, arranjo deslocador de fase (em inglês <i>phase shifter setup</i> , PSS).
DG_τ	Grade de difração do arranjo em 4F que utiliza-se de um arranjo de espelhos do arranjo gerador de atraso (em inglês <i>delay maker setup</i> , DMS).
D_{SMF}	Dispersão cromática das fibras monomodo.
$E(f)$	Sinal óptico criptografado.
f_c	Frequência central.

G_{SMF}	Ganho do amplificador EDFA, para compensar a atenuação do enlace de fibra monomodo.
L_{DCF}	Comprimento do enlace da fibra compensadora de dispersão.
L_{SMF}	Comprimento do enlace de fibra monomodo.
$M(f)$	Sinal elétrico na transmissão.
$M'(f)$	Sinal elétrico descriptado na recepção.
n	Número de fatias espectrais.
N_T	Número mínimo de tentativas.
Rx	Receptor.
$S'_{A\phi\tau}(f)$	Sinal óptico com as fatias espectrais não selecionadas, defasadas e atrasadas, depois de propagar pela rede óptica transparente.
$S'_{\phi\tau}(f)$	Sinal óptico com as fatias já selecionadas, defasadas e atrasadas, após propagar por uma rede óptica transparente.
$S'_{\tau}(f)$	Sinal óptico com as fatias já selecionadas, com as fases complementadas e atrasadas, após propagar pela rede óptica transparente.
$S'(f)$	Sinal óptico com as fatias já selecionadas, com as fases e o atraso compensado, após propagar por uma rede óptica transparente.
$S(f)$	Sinal óptico.
s	Fatia espectral.
$S_A(f)$	Sinal óptico com as fatias espectrais já selecionadas.
$S_{A\phi}(f)$	Sinal óptico com as fatias espectrais selecionadas e defasadas.
$S_{A\phi\tau}(f)$	Sinal óptico com as fatias espectrais já selecionadas, defasadas e atrasadas.
S_{DCF}	Inclinação de dispersão da fibra compensadora de dispersão
SLM_A	SLM em modo de amplitude.
SLM_{ϕ}	SLM em modo de fase.
S_{SMF}	Inclinação de dispersão da fibra monomodo.
Tx	Transmissor.
$X(f)$	Função no domínio da frequência.
$x(t)$	Função no domínio do tempo.

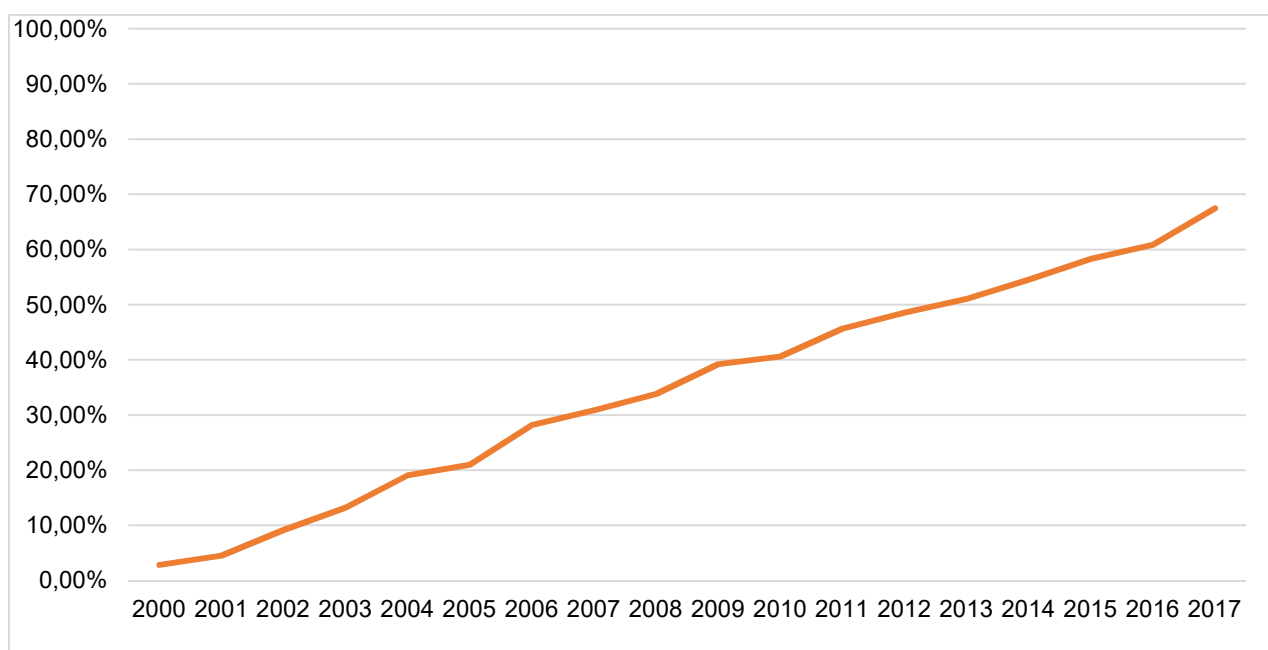
SUMÁRIO

1 INTRODUÇÃO	1
1. 1 Breve Introdução às Comunicações Ópticas	2
1. 2 Segurança em comunicações ópticas	6
1. 3 Encriptação na Camada Física	7
1. 4 Contribuição do Trabalho	8
1. 5 Organização do Trabalho	9
2 DESENVOLVIMENTO	10
2. 1 Configurações de Elementos de Encriptação	11
2. 2 Descrição da Técnica de Encriptação	14
2. 3 Descrição das Simulações	17
2. 3. 1 <i>Transmissores</i>	18
2. 3. 2 <i>Codificador e Decodificador</i>	18
2. 3. 3 <i>Canal Óptico</i>	19
2. 3. 4 <i>Receptores</i>	21
3 RESULTADOS	24
3. 1 Análise dos Resultados para o Canal AWGN B2B	25
3. 2 Análise dos Resultados para o Canal AWGN com 400 km de Propagação	26
3. 3 Comparação dos Dados das Simulações	29
4 CONCLUSÕES	30
REFERÊNCIAS	31

1 INTRODUÇÃO

A União Internacional das Telecomunicações (do inglês *International Telecommunications Union*, ITU) é um órgão responsável por padronizar tecnologias e catalogar dados referentes às telecomunicações. Em 2019, este órgão divulgou dados sobre o crescente número de indivíduos com acesso à Internet de diversos países do mundo todo. Na Figura 1, é ilustrado um gráfico que apresenta o número de brasileiros acessando a Internet ao longo dos primeiros 18 anos deste século (ICTEYE; ITU, 2019). Entre os anos de 2000 até 2017, o Brasil teve um aumento de aproximadamente 65% de usuários na rede. Portanto, mais da metade da população do Brasil, um país com aproximadamente 200 milhões de pessoas (IBGE, 2020) acessa a Internet. Este aumento na rede implica em uma necessidade constante de expansão na sua capacidade, consequentemente na garantia de disponibilizar uma rede segura o suficiente para prover o sigilo das informações transmitidas por ela.

Figura 1 – Brasileiros com acesso à Internet entre os anos de 2000 e 2017



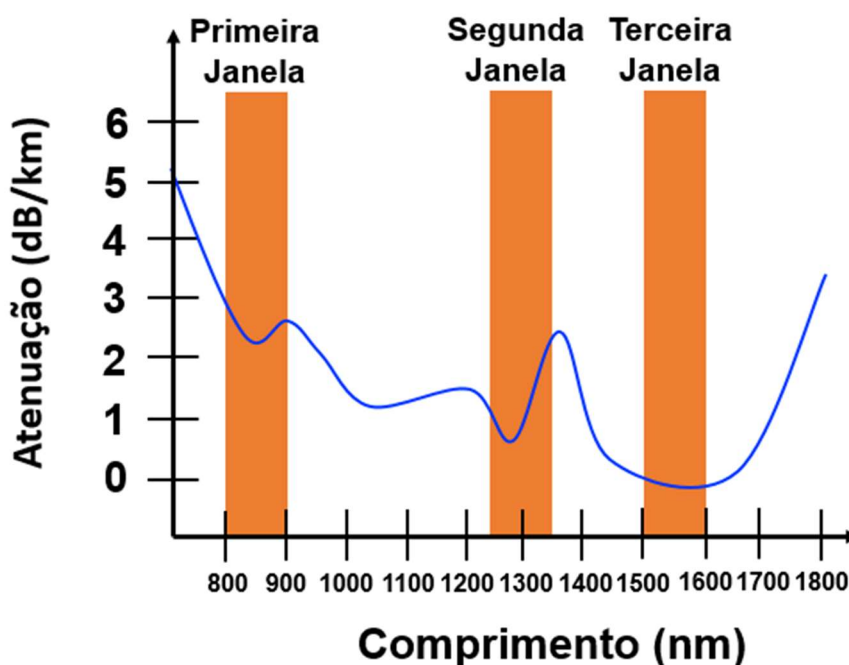
Fonte: Elaborado pelo autor com base em (ICTEYE/ITU, 2019).

1. 1 Breve Introdução às Comunicações Ópticas

Esta seção apresenta uma descrição breve da evolução e do funcionamento das redes que utilizam de comunicação por meio de fibra óptica. É importante mencionar que as comunicações ópticas podem ser realizadas por meios guiados ou não-guiados. Neste trabalho será abordado somente a comunicação óptica por meios guiados, em especial nas fibras ópticas.

A Internet atual é fundamentada nas comunicações ópticas, devido às suas principais vantagens: (i) baixa atenuação, (ii) imunidade a interferências eletromagnéticas e (iii) maior segurança em comparação com outros meios de transmissão (KEISER, 2014). O feixe de luz, que propaga no interior das fibras ópticas, é gerado por meio da amplificação da luz por emissão estimulada de radiação (em inglês *light amplification by stimulated emission of radiation*, LASER). Esses feixes operam, principalmente, em três faixas de comprimento de onda, conhecidas por janelas. As janelas são regiões em que a fibra óptica apresenta os menores valores de atenuação, em relação a determinado comprimento de onda.

Figura 2 – Janelas das comunicações ópticas



Fonte: Elaborado pelo autor com base em (KEISER, 2014).

Por meio do gráfico ilustrado na Figura 2, é possível visualizar o comportamento da atenuação decorrente da fibra óptica no sinal óptico que está propagando no seu interior. A utilização de fibras com atenuação próximas de 0,2 dB/km na faixa de 1550 nm, possibilitou alcançar distancias cada vez maiores nas redes ópticas (RAMASWAMI; SIVARAJAN; SASAKI, 2009). A Tabela 1 traduz os dados, do comportamento da atenuação por quilometro pelo comprimento da onda do sinal, apresentados no gráfico.

Tabela 1 – Relação de comprimento de onda com atenuação, nas janelas do domínio óptico

Janela	Comprimento de onda (nm)	Atenuação (dB/km)
Primeira	800 a 900	3
Segunda	1260 a 1360	0,4
Terceira	1500 a 1600	0,2

Fonte: Elaborado pelo autor com base em (KEISER, 2014).

Os diferentes comprimentos de onda, em que os sinais ópticos operam, são conhecidos como canais. Os canais são organizados conforme a banda de operação, referente aos seus comprimentos de onda, localizados entre 1260 nm e 1675 nm (KEISER, 2014). A divisão das bandas, e a faixa de comprimento de onda em que localizam-se é apresentado na Tabela 2, sendo que O, E, S, C, L e U referem-se, respectivamente às nomenclaturas em língua inglesa: *original*, *extended*, *short*, *conventional*, *long* e *ultra-long* (BOBADILLA, 2018).

Tabela 2 – Comprimento de onda das bandas espectrais utilizadas em comunicações ópticas

Banda	Comprimento de onda (nm)
O	1260 a 1360
E	1360 a 1460
S	1460 a 1530
C	1530 a 1565
L	1565 a 1625
U	1625 a 1675

Fonte: Elaborado pelo autor com base em (BOBADILLA, 2018).

Outra tecnologia, crucial nas comunicações ópticas, é o formato da modulação do sinal. A modulação tem como objetivo alcançar a melhor performance possível do sinal, na sua taxa de transmissão e faixa de operação operante.

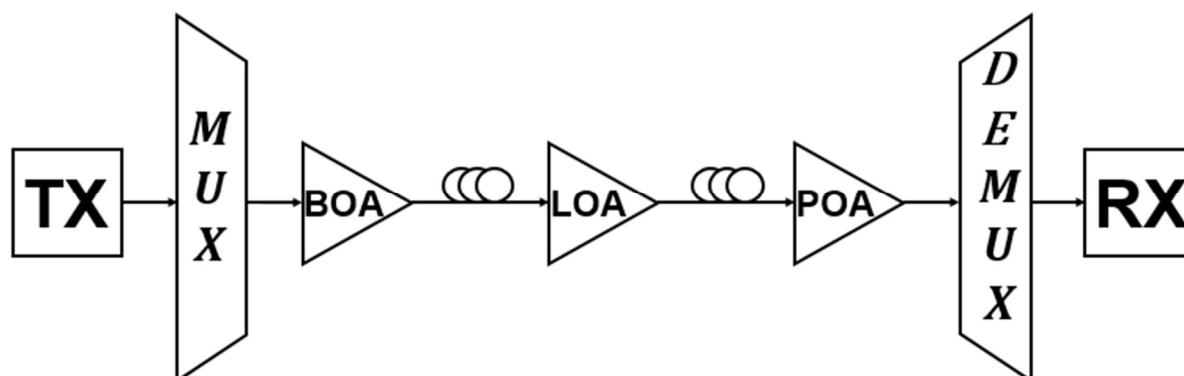
A modulação mais simples, presente nas redes ópticas, é a modulação de chaveamento liga e desliga (em inglês *on-off keying*, OOK) (LATHI; DING, 2012). A modulação OOK, é realizada por meio de chaveamento de amplitude (em inglês *amplitude shift keying*, ASK), em que a informação do sinal é transmitida por dígitos binários (do inglês *binary digit*, bit), representados pela ausência de pulsos, bit 0, e a presença de pulso, bit 1.

O aumento da demanda por tráfego de rede necessitou de diferentes formatos de modulação, capazes de suportar taxas de transmissão cada vez maiores. Em vez de utilizar o ASK, essas modulações realizam o chaveamento de fase (em inglês *phase shift keying*, PSK). A modulação que utiliza PSK mais simples é a modulação de chaveamento de fase binário (em inglês *binary phase shift keying*, BPSK).

A BPSK detecta a diferença de bit por meio da defasagem presente na onda portadora, quando a fase está em 0° , o bit é 0, quando a fase está em 180° , o bit é 1. Outra modulação em PSK, que suporta taxas de transmissão maiores que a BPSK, é a modulação QPSK. O funcionamento das duas modulações de PSK são parecidos, porém, a QPSK utiliza quadratura de fase, ou seja, ela transmite uma diferente informação em 0° , 90° , 180° e 270° , com um diferente par de bits a cada alteração de fase, dois bits a cada símbolo.

Existe a possibilidade de multiplexar dois sinais modulados em QPSK, que devem ter suas polarizações ortogonais uma à outra, gerando uma modulação conhecida por chaveamento de fase em quadratura com dupla polarização (em inglês *dual-polarization quadrature phase shift keying*, DP-QPSK). Por ser uma dupla polarização de um sinal modulado em QPSK, o sinal em DP-QPSK tem quatro bits por símbolo, dobrando a eficiência espectral.

Figura 3 – Amplificadores, multiplexador e demultiplexador óptico



Fonte: O autor (2020).

A Figura 3 ilustra a posição de cada um dos dispositivos presentes em uma rede de comunicação por fibra óptica, em que TX é o transmissor e RX o receptor. A necessidade do aumento da capacidade da infraestrutura das redes de comunicações ópticas, impulsionaram o desenvolvimento de dispositivos ópticos que conseguissem convergir diferentes comprimentos de onda em apenas uma fibra óptica como os multiplexadores ópticos (MUX). Um dispositivo oposto ao multiplexador também foi necessário, um dispositivo óptico capaz de separar os diferentes comprimentos de onda, o demultiplexador óptico (DEMUX). Os dispositivos ópticos citados viabilizaram o desenvolvimento da multiplexação por divisão de comprimento de onda (em inglês *wavelength division multiplexing*, WDM) (KEISER, 2014; AGRAWAL, 2014), permitindo a transmissão simultânea de diferentes sinais ópticos, operando em diferentes comprimentos de onda, por meio de apenas uma única fibra óptica. Inicialmente, as redes ópticas utilizavam-se somente de regeneradores, dispositivos que por meio de conversão electro-óptica, que reamplificam, reformatam e retemporizam o sinal óptico. Porém, devido ao alto custo desses dispositivos eles foram amplamente substituídos por amplificadores ópticos que permitem, de forma transparente, amplificar os sinais ópticos sem conversão electro-óptica assim compensando a atenuação acumulada e viabilizando propagação por um número cada vez maior de enlaces na rede. Quando os amplificadores são utilizados na saída do dispositivo que realiza a multiplexação óptica, eles são chamados de amplificadores de potência (em inglês *booster optical amplifier*, BOA). Se eles forem utilizados entre nós de uma rede óptica, serão chamados de amplificadores de linha (em inglês *line optical amplifier*, LOA). Os amplificadores utilizados na recepção do

dispositivo que realiza a demultiplexação óptica, são chamados de pré-amplificador (em inglês *pre-optical amplifier*, POA). Amplificadores ópticos também podem ser agrupados conforme à sua técnica de amplificação: (i) amplificadores Raman, em que a amplificação é realizada por meio do efeito não-linear Raman e (ii) amplificadores com fibra dopada à érbio (em inglês *erbium-doped fiber amplifier*, EDFA), em que a amplificação é realizada pela emissão espontânea dos átomos de érbio presentes na fibra no interior do dispositivo.

As tecnologias descritas até este ponto, junto à implementação de tecnologias como, correção antecipada de erro (em inglês *forward error correction*, FEC) e processamento digital de sinais (em inglês *digital signal processing*, DSP), podem viabilizar taxas de transmissão comerciais de até 400 Gb/s (JIA; CHIEN; ZHANG; CAI; YU, 2015; KONG, 2019), ou até mesmo 600 Gb/s (KONG, 2019). Recentemente a empresa estadunidense Infinera, divulgou a notícia que obteve a taxa de transmissão de 800 Gb/s por canal, propagado em uma rede óptica de 950 km (INFINERA, 2020).

1. 2 Segurança em Comunicações Ópticas

Anualmente são gastos mais de US\$100 bilhões para garantir maior segurança na rede (GARTNER, 2018). A transmissão dos sinais em feixes de luz, no interior dos cabos de fibra óptica, proporcionam uma segurança ainda maior, principalmente em relação à outras tecnologias de telecomunicações (KEISER, 2014). Por mais que sejam realizados esses esforços, para garantir a segurança da rede, em 2013 foi explanado, pelo ex-funcionário da Agência Nacional de Segurança do Governo Estadunidense (do inglês *National Security Agency*, NSA), Edward Snowden que a NSA, junto ao Quartel General de Comunicação do Governo Britânico (do inglês *Government Communications Headquarters*, GCHQ), que essas organizações espionavam o conteúdo das fibras ópticas (BBC, 2014; THE GUARDIAN, 2013). A violação das fibras foi possível por meio de dispositivos, que de maneira não intrusiva, desviam o feixe de luz de dentro da fibra óptica (IQBAL; FATHALLAH; BELHADJ, 2012), chamados de grampos ópticos passivos (em inglês *passive fiber clip-on coupler*). Infelizmente esses problemas de segurança sempre existirão, pois seria necessário inspecionar todas as fibras presentes na rede óptica, o que tornaria os custos da manutenção do sistema muito altos. Portanto, a única solução é mitigar os

custos, utilizando-se de encriptações, impossibilitando que o invasor (em inglês *eavesdroper*) entenda a informação (PONEMON INSTITUTE/IBM SECURITY, 2018).

As técnicas de encriptação, foram inicialmente reservadas para aplicação na sexta camada (camada de apresentação) do modelo para interconexão de sistemas abertos (do inglês *open system for interconnections*, OSI) (TANENBAUM, 2011). Porém, o maior número de camadas encriptadas reforça em uma maior segurança na informação (KITAYAMA, 2011). O feixe de luz, que transmite a informação nas comunicações ópticas, está presente na primeira camada (camada física) do modelo OSI, e é a criptografia desta camada em que consiste o tema deste trabalho.

1. 3 Encriptação na Camada Física

A seguir, a discussão é focada na relação de algumas técnicas de criptografia aplicadas à camada física. Um exemplo de técnica aplicável na primeira camada, não restrita às comunicações ópticas, são as criptografias caóticas (GOEDGEBUER, 2002), em que a portadora de um sinal óptico, gerada por meio de um LASER na transmissão, encripta a informação que será descriptada por meio de um segundo LASER sincronizado com o primeiro. A principal desvantagem desta técnica é a falta de sincronia entre ambos os LASERs, pois os longos enlaces de fibra óptica dificultam a sincronização (ABBADÉ, 2013).

Outro método de encriptar o sinal nas comunicações ópticas, é a criptografia quântica (SINGH, 2001; KARTALOPOULOS, 2007; LYDIA; SMAIL; MOHAMED, 2017). Este método é considerado eficiente, porém encontra-se ainda em fase de desenvolvimento e apresenta algumas desvantagens. Sendo essas desvantagens o seu custo elevado (LYDIA; SMAIL; MOHAMED, 2017) e aplicação limitada a aproximadamente 100 km (KARTALOPOULOS, 2007). O seu funcionamento baseia-se na linearidade da polarização de fótons individuais (SINGH, 2001), transmitidos por uma fibra óptica.

Outra tecnologia que viabiliza a encriptação do sinal, na camada física, é o acesso múltiplo por divisão de código óptico (em inglês *optical code division multiple access*, OCDMA) (KOSTINSKI; KRAVTSOV; PRUCNAL, 2008; WANG; WADA, 2007; WANG, 2007), que possibilita a comunicação em sincronia, e simultânea, de diversas duplas de usuários, em que, cada par utiliza de uma cifra exclusiva. Por mais que a

OCDMA permite uma encriptação na transmissão, ela provoca o indesejado alargamento da banda de operação do sinal óptico criptografado.

Técnicas criptográficas baseadas no uso de portas OU exclusivas ópticas (do inglês *optical OR exclusive gate*, XOR ópticas) podem operar em um ambiente livre de interferências eletromagnéticas com altas taxas de transmissão (BOBADILLA, 2018; DAHAN; MAHLAB, 2017). Por meio da modulação cruzada de polarização (do inglês *cross polarization modulation*, XPoLM) (SOTO; ERASME; GUEKOS, 2001), modulação cruzada de fase (do inglês *cross-phase modulation*, XPM) (KIM; JHON; BYUN; LEE; WOO; KIM, 2002) e a mistura de quatro ondas (em inglês *four wave mixing*, FWM) (ZHANG; CUI; ZHAN; ZHANG; CHEN, 2015), foi possível aplicar técnicas baseadas nas XOR ópticas. Essas técnicas são eficientes, porém com exceção da FWM, operam somente junto à modulação OOK, impossibilitando à aplicação em diferentes modulações.

Em redes ópticas transparentes (em inglês *transparent optical networks*, TON) é possível implementar uma técnica que realiza a criptografia por meio de codificação espectral de fase (do inglês *spectral phase encoding*, SPE). O processo de encriptação é realizado ao dividir um sinal óptico em n fatias espectrais, sendo que, cada uma dessas fatias recebe um deslocamento único na fase. Durante o processo de descriptação a fase é alterada mais uma vez, de modo que cada uma das fatias seja deslocada em um valor de fase complementar, em relação à encriptação. Em virtude de melhorar a robustez da SPE, foi proposta a criptografia por codificação espectral de fase e atraso (do inglês *spectral phase and delay encoding*, SPDE) (BOBADILLA, 2018; ABBADE, 2017). A SPDE é muito similar à SPE, o que às difere é o atraso temporal aplicado nas fatias espectrais na técnica SPDE (ABBADE, mai. 2015; ABBADE, jul. 2015). O atraso aplicado permite o aumento da robustez na técnica de encriptação.

1. 4 Contribuição do Trabalho

Este trabalho é uma evolução da técnica de codificação óptica por meio de embaralhamento espectral multi-canal (em inglês *All-Optical Encryption Using Multi-Channel Spectral Shuffling*, AOSS) (BOBADILLA, 2018; ABBADE; BOBADILLA; DE CARVALHO; FERREIRA; BONANI; ALDAYA, 2019). Esta técnica realiza uma divisão

do sinal óptico em n fatias espectrais e as encripta por meio do embaralhamento entre todas essas fatias. Desta forma, se um invasor estiver desviando um feixe de luz para espionar a informação contida, será preciso monitorar todos os canais ópticos encriptados simultaneamente para que seja possível descriptrar a informação, dificultando o trabalho do invasor. Porém é possível tornar a AOSS ainda mais complexa, deslocando a fase e realizando um atraso temporal em cada uma das n fatias espectrais do sinal óptico, que é a técnica criptográfica proposta neste trabalho. A técnica permite ser implementada em situações em que é necessário maior segurança das redes ópticas.

1. 5 Organização do Trabalho

Neste capítulo apresentamos os fundamentos básicos para compreensão da importância do uso das comunicações ópticas nas redes atuais, que demandam altas taxas de transmissão, uma introdução dos conceitos relacionados à criptografia, juntamente à necessidade do seu uso, e como é a sua aplicação nas redes ópticas. O restante deste trabalho está organizado da seguinte maneira, o segundo capítulo descreve o funcionamento da técnica abordada, e em seguida, os parâmetros aplicados nas simulações, referidas aos arranjos da técnica previamente explicitada. As análises realizadas e os resultados obtidos, são apresentados no terceiro capítulo. A conclusão, e demais considerações finais, são discutidas no quarto e último capítulo.

2 DESENVOLVIMENTO

Neste trabalho, é convencionado que as funções representadas em letra minúscula, como $x(t)$, referem-se ao domínio do tempo, enquanto as funções escritas com letras maiúsculas são referentes ao domínio da frequência, como $X(f)$. Além disso, fica subentendido que a transformada de Fourier de $x(t)$ é $X(f)$ (LATHI; DING, 2012). Observa-se que o trabalho a seguir é uma evolução daquele apresentado em (BOBADILLA, 2018).

Para realizar a criptografia em dois sinais ópticos, a técnica utiliza a divisão espectral desses sinais em n fatias espectrais. Para facilitar a explicação da técnica de criptografia, em questão, considera-se que $n = 7$. No entanto, observa-se que esse número pode ser muito maior, de fato, as simulações apresentadas no Capítulo 3 operam com até 330 fatias. O número de fatias espectrais escolhido é importante para dificultar ataques de força bruta, pois este tipo de ataque exige que o invasor realize um número de tentativas proporcional ao número de fatias para quebrar o padrão da criptografia. Desta forma, quanto maior o número de fatias espectrais, mais robusta é a técnica de encriptação. Por meio de:

$$N_T = 2^n \quad (1)$$

em que N_T é o número mínimo de tentativas para que um invasor consiga recuperar o sinal (ABBADE; BOBADILLA; DE CARVALHO; FERREIRA; BONANI; ALDAYA, 2019), é possível verificar a robustez da técnica em relação ao número de fatias espectrais que o sinal será dividido. Porém, o número mínimo de tentativas pode ser ainda maior quando o padrão dessas fatias é alterado. Na técnica desenvolvida essa alteração de padrão é feita de duas formas, primeiro, por meio de alteração de fase de cada uma das fatias espectrais, em que é possível estimar o número mínimo de tentativas por meio de:

$$N_T = (n)^{\frac{360}{\Delta\theta}} \quad (2)$$

em que $\Delta\theta$ representa o erro máximo que um invasor pode ter ao tentar acertar a fase de uma fatia espectral (SANTOS, 2020). Logo é possível combinar a Equação 1 com a Equação 2, resultando em:

$$N_T = 2^n \cdot (n)^{\frac{360}{\Delta\theta}} \quad (3)$$

que estima um número mínimo de tentativas quando o sinal óptico tem suas fatias espectrais embaralhadas e defasadas. A segunda alteração é o alargamento de pulso, que consiste em um atraso específico em cada uma das fatias espectrais. Não há um cálculo que defina o número mínimo de tentativas quando há o atraso aplicado nas fatias, porém isso pode ser estudado em novo trabalho.

2. 1 Configurações de Elementos de Encriptação

Durante o processo da criptografia será necessário o uso de três diferentes configurações de elementos dispostos em um arranjo 4F. Esse nome advém do fato de o arranjo conter 4 elementos e de todos estarem espaçados pela distância focal F é de dois dos elementos, que são lentes esférica convergentes (em inglês *convergent spherical lens*, CSL).

Duas das configurações dos arranjos em 4F fazem o uso de moduladores espaciais de luz (do inglês *spatial light modulator*, SLM). Os SLMs são compostos por uma matriz de *pixels*, como em uma tela de cristal líquido (em inglês *liquid crystal display*, LCD). É possível operar o SLM em dois modos, ambos usados nesse trabalho. No primeiro modo, que será chamado de modo de amplitude, a aplicação de uma tensão a um dado *pixel* controla a intensidade da luz que emerge desse *pixel*. Assim, é possível bloquear a passagem da luz ou permitir a transmissão de uma intensidade máxima. No segundo modo, designado por modo de fase, a variação da tensão entre os terminais de um *pixel* controla a fase da luz emergente.

O arranjo em 4F com um modulador SLM operando no modo de amplitude é chamado de arranjo divisor de fatias (em inglês *spectral slicer setup*, SSS) e ilustrado na Figura 4, seu funcionamento é descrito nos itens a seguir:

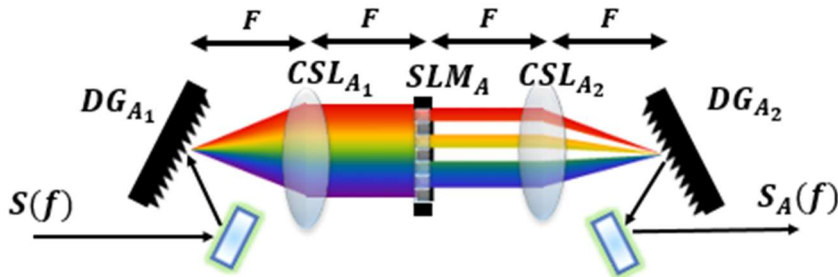
1. O sinal óptico que propaga por este arranjo, primeiramente, incide em uma grade de difração (do inglês *diffraction grating*, DG). Na Figura 4 o

sinal $S(f)$ é difratado por uma grade denominada DG_{A_1} e transmitido por uma lente esférica convergente CSL_{A_1} .

2. Em seguida $S(f)$ atravessa um modulador espacial de luz, que está operando em amplitude, SLM_A . O conjunto das componentes espectrais que emerge de cada *pixel* é chamado de fatia espectral. No exemplo ilustrado na Figura 4, o SLM_A permitiu a passagem de 4 das 7 fatias espectrais de $S(f)$, respectivamente s_1, s_2, s_3 e s_4 .
3. A próxima lente esférica convergente CSL_{A_2} , converge o sinal em direção à grade de difração DG_{A_2} que, por sua vez, colima as fatias espectrais em um novo sinal, $S_A(f)$.

Observa-se que as fatias são criadas no domínio espacial, mas que cada *pixel* atua sobre um conjunto específico de componentes espectrais, que são multiplexadas por DG_{A_2} . Assim, é conveniente chamar essas fatias de fatias espectrais.

Figura 4 – Arranjo divisor de fatias (em inglês *spectral slicer setup*, SSS), operando com SLM em modo de amplitude



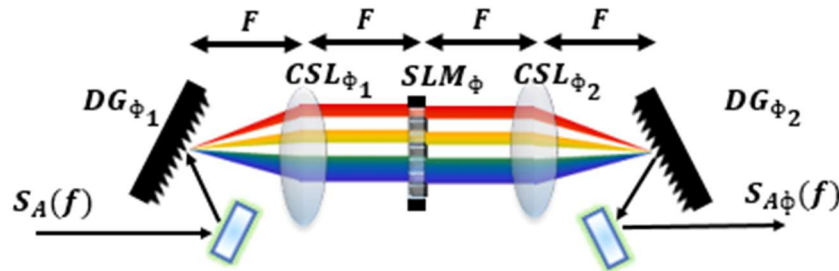
Fonte: O autor (2020).

O modulador espacial de luz, operando em modo de fase em um arranjo em $4F$, é chamado de arranjo deslocador de fase (em inglês *phase shifter setup*, PSS) e está ilustrado na Figura 5. O seu funcionamento está descrito nos itens abaixo:

1. O sinal óptico $S_A(f)$ passa por uma grade de difração, DG_{ϕ_1} , e por uma lente esférica convergente CSL_{ϕ_1} . Até aqui, o processo é o mesmo daquele descrito no item 1 do modo de operação em amplitude.;

2. O sinal que emerge de CSL_{ϕ_1} atravessa o SLM SLM_{ϕ} . Assim, cada uma das quatro fatias espectrais de $S_A(f)$ recebem deslocamentos de fase de ϕ_i ($i= 1, 3, 5$ e 6);
3. Como no caso do modo de amplitude, o sinal na saída do SLM convergido por uma lente esférica CSL_{ϕ_2} , e suas fatias são multiplexadas ao passar pela grade de difração DG_{ϕ_2} , resultando assim no sinal $S_{A\phi}(f)$.

Figura 5 – Arranjo deslocador de fase (em inglês *phase shifter setup*, PSS), operando com o SLM em modo de fase



Fonte: O autor (2020).

O terceiro arranjo 4F, arranjo gerador de atraso (em inglês *delay maker setup*, DMS), utiliza espelhos espaçados entre si por uma distância ajustável. Esses espelhos são dispostos para prover atrasos distintos a cada fatia espectral, por meio de:

$$\tau_i = \frac{d_i}{c} \quad (4)$$

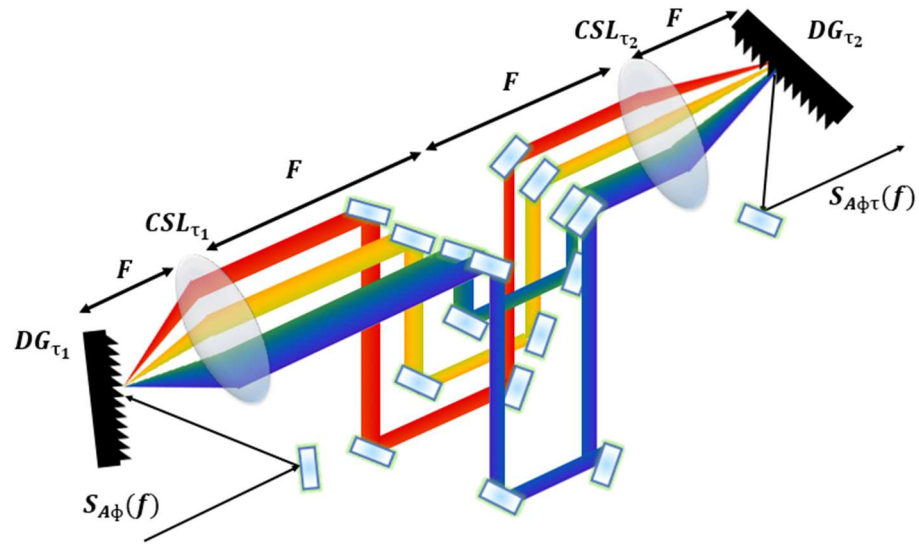
em que: (i) c é a velocidade da luz no vácuo, igual a 299 792 458 m/s, (ii) τ_i equivale ao atraso específico ($i= 1, 2, \dots, n$) aplicado à i -ésima fatia e (iii) d_i é a distância entre os espelhos ($i= 1, 2, \dots, n$) associados à i -ésima fatia.

A disposição desse arranjo em 4F, chamado de arranjo 4F no modo atraso, é ilustrada na Figura 6. O modo de operação desta disposição em 4F é descrita a seguir:

1. O sinal óptico $S_{A\phi}(f)$ é difratado pela grade de difração DG_{τ_1} e em seguida direcionado para a lente esférica CSL_{τ_1} ;

2. Cada uma das fatias do sinal $S_{A\phi}(f)$ percorre uma distância d_i no arranjo de espelhos, recebendo um atraso específico, designando-se por τ_1 , τ_2 , τ_3 e τ_4 ;
3. Após essa operação CSL_{τ_2} colima o sinal óptico em sua entrada e a grade de difração DG_{τ_2} gera o sinal $S_{A\phi\tau}(f)$, com as fatias multiplexadas.

Figura 6 – Arranjo gerador de atraso (em inglês *delay maker setup*, DMS), operando com um arranjo de espelhos



Fonte: O autor (2020).

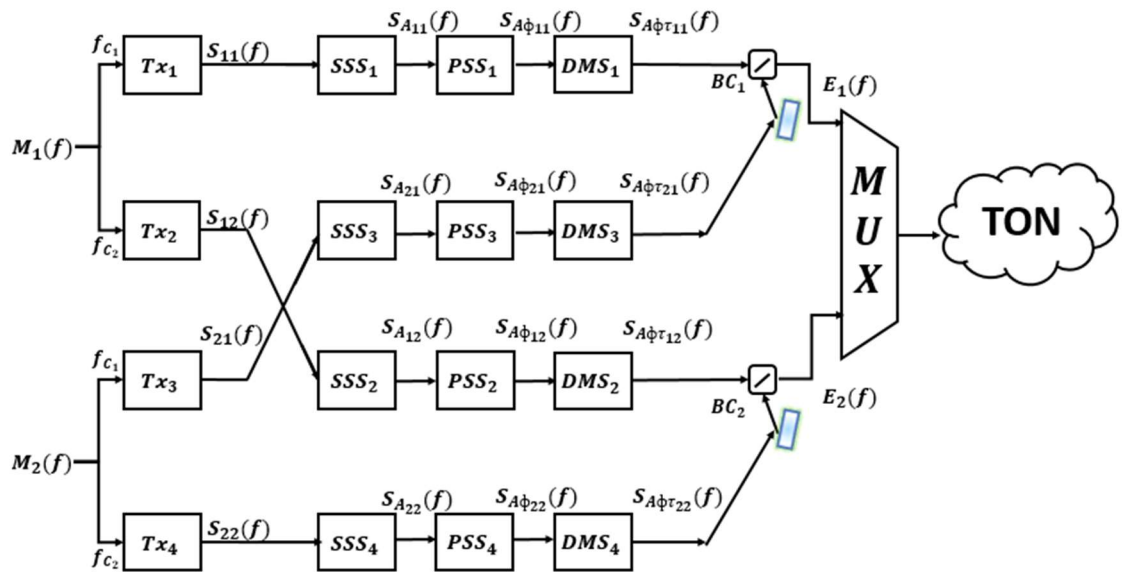
2. 2 Descrição da Técnica de Encriptação

O método de encriptação usado nesse trabalho é o mesmo de (BOBADILLA, 2018), acrescido de uma etapa para encriptação de fase. A Figura 7 apresenta um diagrama de blocos para esse processo, cujas principais etapas são:

1. O sinal elétrico $M_1(f)$ é modulado para o domínio óptico pelos transmissores ópticos T_{x_1} e T_{x_2} , com frequências centrais f_{c_1} e f_{c_2} , respectivamente, gerando assim os sinais $S_{11}(f)$ e $S_{12}(f)$. Um segundo sinal elétrico, $M_2(f)$, também é modulado em f_{c_1} e f_{c_2} , gerando os sinais ópticos $S_{21}(f)$ e $S_{22}(f)$, respectivamente. Durante a discussão os sinais ópticos são generalizados por $S_{jk}(f)$ ($j = 1$ ou 2 e $k = 1$ ou 2);

2. Cada um dos sinais ópticos representados por $S_{jk}(f)$ propagam por um SSS para selecionar as fatias espectrais desses sinais. Na saída dos divisores de fatias nomeamos os sinais ópticos resultantes por $S_{A_{jk}}(f)$;
3. Cada fatia dos sinais ópticos é deslocada em fase pelo PSS que está em seguida do SSS, em relação ao percurso do sinal. O sinal óptico que é multiplexado na saída do PSS é designado por $S_{A\phi_{jk}}(f)$;
4. Os sinais ópticos com suas fatias espectrais deslocadas em fase passam por um DMS que aplica um atraso em cada uma dessas fatias. Os sinais ópticos resultantes do arranjo gerador de atraso são referidos por $S_{A\phi\tau_{jk}}(f)$;
5. Tendo todos os sinais ópticos com suas fatias espectrais deslocadas na fase e no tempo, os sinais $S_{A\phi\tau_{11}}(f)$ e $S_{A\phi\tau_{21}}(f)$ são multiplexados por um combinador de feixe (em inglês *beam combiner*, BC) BC_1 e assim são embaralhados, gerando o sinal óptico criptografado $E_1(f)$. Os sinais ópticos $S_{A\phi\tau_{12}}(f)$ e $S_{A\phi\tau_{22}}(f)$ são também multiplexados, porém pelo combinador de feixe BC_2 , embaralhando as fatias espectrais de ambos os sinais combinados e gerando o sinal óptico criptografado $E_2(f)$.
6. Após sua origem, os sinais ópticos criptografados $E_1(f)$ e $E_2(f)$ são multiplexados por um multiplexador óptico, e propagados por uma TON.

Figura 7 – Processo de encriptação do sinal óptico



Fonte: O autor (2020).

Após a propagação pela TON, é necessário descriptar o sinal. Na Figura 8 é ilustrado este procedimento. Os itens referentes à decodificação possuem similaridades em alguns pontos de (BOBADILLA, 2018).

7. O sinal óptico vindo da TON chega na entrada do demultiplexador e é demultiplexado em dois diferentes sinais ópticos ainda embaralhados e criptografados $E_1(f)$ e $E_2(f)$, que operam nas frequências f_{c_1} e f_{c_2} , respectivamente;
8. Após a passagem pelo demultiplexador, o sinal óptico $E_1(f)$ passa por um divisor de feixe (em inglês *beam splitter*, BS) BS_1 , que o divide em dois sinais $S'_{A\phi\tau_{11}}(f)$ e $S'_{A\phi\tau_{21}}(f)$. Um processo análogo ocorre para o sinal $E_2(f)$, que ao passar por BS_2 é dividido em $S'_{A\phi\tau_{12}}(f)$ e $S'_{A\phi\tau_{22}}(f)$. Com o intuito de simplificar as representações dos sinais ópticos, os nomearemos por $S'_{A\phi\tau_{jk}}(f)$ ($j = 1$ ou 2 e $k = 1$ ou 2);
9. Cada um dos sinais ópticos vindo do divisor de feixe passa por um SSS que vai selecionar as fatias espectrais relativas às fatias que foram selecionadas no primeiro arranjo divisor de fatias. Os sinais ópticos $S'_{A\phi\tau_{jk}}(f)$ ao propagarem pelo SSS de seu devido percurso, geram respectivamente, os sinais ópticos $S'_{\phi\tau_{jk}}(f)$;
10. Os sinais que emergiram dos arranjos divisores de fatias percorrem em seguida um PSS. O deslocamento de fase aplicado em cada uma das fatias ϕ'_i ($i = 1, 2, \dots, n$) será o complemento para 360° com relação ao deslocamento ϕ , Equação 5:

$$\phi'_i = 360 - \phi \quad (5)$$

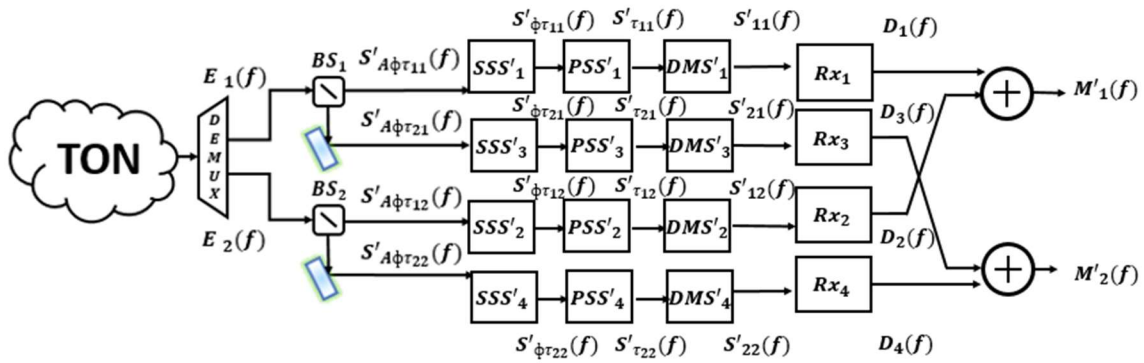
Pois assim a defasagem gerada no primeiro grupo de arranjos deslocadores de fase será compensada. Com o deslocamento de fase compensado dos sinais ópticos $S'_{\phi\tau_{jk}}(f)$ os sinais $S'_{\tau_{jk}}(f)$ são gerados;

11. Tendo as fatias desembaralhadas e compensadas em fase, a última etapa da decodificação é corrigir o atraso aplicado antes da propagação dos sinais pela TON, τ_i . Para compensar o atraso da encriptação será

aplicado um novo atraso que equaliza todas as fatias espectrais no domínio do tempo. Assim os sinais representados por $S'_{\tau_{jk}}(f)$ foram equalizados no tempo e deram origem aos sinais ópticos $S'_{11}(f)$, $S'_{12}(f)$, $S'_{21}(f)$ e $S'_{22}(f)$;

12. Os sinais ópticos $S'_{11}(f)$ e $S'_{12}(f)$, captados pelos receptores R_{X_1} e R_{X_3} , respectivamente, são demodulados e retornados à banda-base. Os sinais demodulados são acoplados por um acoplador que gera o sinal decodificado $M'_1(f)$. Os sinais ópticos $S'_{21}(f)$ e $S'_{22}(f)$ passam pelas mesmas etapas, porém nos receptores R_{X_2} e R_{X_4} , respectivamente, gerando assim o sinal decodificado $M'_2(f)$.

Figura 8 – Processo de descriptação de um sinal óptico



Fonte: O autor (2020).

2. 3 Descrição das Simulações

A análise e o desenvolvimento das simulações foram feitos por meio do *software* VPI. A escolha do *software* se deve aos fatos desse *software*: (i) ser específico para simulações de sistemas ópticos, (ii) ter uma vasta biblioteca de componentes para simulação de processamento óptico e digital de sinais, (iii) ser reconhecido como uma plataforma confiável de simulação, cujos resultados podem reproduzir de maneira adequada aqueles obtidos em laboratório e em testes de campo e (iv) à familiaridade que os integrantes de nossa equipe desenvolveram com esse *software*. Em conjunto, todos esses elementos favoreceram a simulação da técnica descrita neste trabalho no referido *software*.

2. 3. 1 Transmissores

Seguindo o diagrama de blocos apresentado na Figura 7, que apresenta o processo de encriptação do sinal óptico da técnica descrita, possui quatro transmissores T_{x_1} , T_{x_2} , T_{x_3} e T_{x_4} , contendo os seguintes parâmetros:

1. Os sinais elétricos convertidos em sinais ópticos pelos transmissores possuem uma sequência binária pseudoaleatória (do inglês *pseudorandom bit sequence*, PRBS) de 2^{18} bits de comprimento;
2. Cada transmissor realiza a modulação por QPSK, com uma taxa de transmissão de 56 Gb/s;
3. Em T_{x_1} e T_{x_3} a frequência das portadoras é de 193,05 THz enquanto de T_{x_2} e T_{x_4} as portadoras são de 193,15 THz. Assim entre cada sinal óptico a ser criptografado pelo codificador, há um espaçamento de 100 GHz;
4. A potência média emitida pelo LASER é de 1,65 mW;
5. Também há a presença de filtro de Nyquist, com um fator de decaimento (do inglês *roll-off*) de 0,1, utilizado para deixar o perfil espectral do sinal mais plano, ou seja, com potência uniformemente distribuídas no intervalo de 0,9 a 1,1 da banda mínima (por meio dos parâmetros empregados neste trabalho, a banda mínima mencionada equivale a 14 GHz, logo o intervalo varia de 12,6 a 15,4 GHz) das componentes espectrais. Assim quando o sinal tiver for dividido em fatias, a potência de cada fatia espectral será aproximadamente a mesma.

2. 3. 2 Codificador e Decodificador

Os arranjos de SLMs, conjuntos de dispositivos que realizam a criptografia, foram emulados no *software* VPI, por meio de:

1. Filtros passa-faixa, para selecionar quais fatias espectrais serão bloqueadas do sinal;

2. Multiplexadores, para multiplexar os sinais ópticos;
3. Demultiplexadores, que realizam a dispersão espacial do sinal.

O parâmetro que indica a porcentagem de luz transmitida dentro de cada *pixel* do SLM é o fator de preenchimento (do inglês *fill-factor*). Nos equipamentos disponíveis no mercado o fator de preenchimento típico é de 98%. Isso significa que 98% da luz é transmitida pela SLM e os 2% restantes são bloqueados por zonas opacas existentes entre as bordas que delimitam cada um dos *pixels*. Para simular este parâmetro nos filtros passa-faixa o fator de preenchimento é representado por uma constante que multiplica cada uma das larguras de banda dos filtros.

Para analisar a influência da quantidade de fatias junto à técnica da criptografia, foram feitas simulações com diferentes larguras de banda, sendo elas: 0,24 GHz para 128 fatias, 0,12 GHz para 256 fatias e 0,09 GHz para 330 fatias. Nas situações mencionadas foram utilizados filtros passa-faixa para criar as fatias a passarem pelo embaralhador. Após embaralhado o sinal passa por um deslocamento de fase que varia de 0 a 360 graus, além de um atraso de 0 a 20 períodos por símbolo (a taxa de transmissão e a modulação utilizadas no estudo deste trabalho, implicam que, um período de símbolo equivale a 35,714286 ps).

2. 3. 3 Canal Óptico

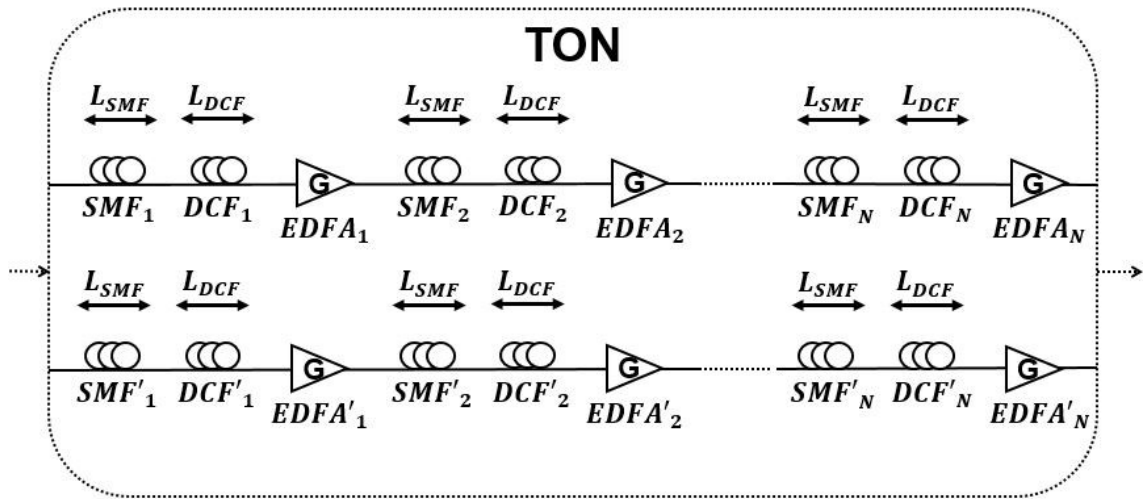
Para melhor avaliação do desempenho da técnica em uma rede óptica transparente, dois canais ópticos diferentes foram desenvolvidos para as simulações.

A primeira configuração, mais simples, possui um ruído gaussiano aditivo branco (do inglês *additive white gaussian noise*, AWGN) inserido no canal que é ligado diretamente da saída do codificador à entrada do decodificador, caracterizando um sistema, do inglês, *back-to-back* (B2B).

Na segunda configuração, como apresentado no diagrama de blocos da Figura 9, mais uma vez um canal com AWGN é utilizado. Porém, nesta situação existem enlaces de fibra óptica conectando a saída do codificador com a entrada do decodificador. Os enlaces foram divididos por um demultiplexador na saída do codificador em dois caminhos idênticos, compostos por enlaces de fibra monomodo (do inglês *single mode fiber*, SMF), de comprimento L_{SMF} e fibra compensadora de dispersão (do inglês *dispersion compensation fiber*, DCF), de comprimento L_{DCF} para

compensar a dispersão acumulada ao longo da propagação (KEISER, 2014). Entre cada enlace se fez a utilização de um EDFA, com um ganho G_{SMF} , que compensa a atenuação decorrente à propagação do sinal na fibra. Esse tipo de amplificador emite ruído de emissão espontânea amplificada (do inglês *amplified spontaneous emission*, ASE) (KEISER, 2014) que degrada a qualidade dos sinais amplificados.

Figura 9 – Diagrama de blocos do canal óptico do arranjo



Fonte: O autor (2020).

A dispersão cromática a ser compensada, devido à propagação do sinal nas fibras monomodo, define o comprimento da DCF, determinado por meio de:

$$L_{DCF} = \frac{D_{SMF} \cdot L_{SMF}}{|D_{DCF}|} \quad (6)$$

em que D_{DCF} é a dispersão cromática das fibras compensadoras de dispersão em ps/nm.km. A dispersão cromática da SMF, representada por D_{SMF} , também é aplicada em ps/nm.km. O comprimento total do enlace da fibra monomodo, L_{SMF} , é calculada em km.

O ganho G_{SMF} , necessário para que o EDFA realize a compensação da atenuação devido à propagação do sinal nas SMF, é determinado por:

$$G_{SMF} = L_{SMF} \cdot \alpha_{SMF} \quad (7)$$

em que α_{SMF} , em dB/km, é a atenuação mencionada.

A Tabela 3 apresenta os valores de cada um dos parâmetros existentes na TON emulada no *software* VPI, por percurso, como ilustrado na Figura 9. Cada uma das rotas possui um comprimento de 400 km, caracterizando uma rede de longa distância (do inglês *wide area network*, WAN). Por meio deste arranjo é possível evitar a influência da diafonia (em inglês *crosstalk*), pois apenas um único canal é propagado por cada caminho. Em trabalhos futuros pode ser interessante estudar o comportamento do sinal propagado com a presença de diafonia.

Tabela 3 – Parâmetros dos elementos existentes na TON do arranjo

Parâmetro	Valor
Comprimento total de cada conjunto de enlaces SMF (km)	400
Quantidade de enlaces no arranjo	5
Comprimento de cada enlace SMF L_{SMF} (km)	80
Dispersão cromática da SMF D_{SMF} (ps/nm.km)	16
Inclinação de dispersão (S_{SMF}) da SMF (s/m ³)	80
Parâmetro não-linear da SMF (m ² /W)	$10 \cdot 10^{-20}$
Atenuação da SMF α_{SMF} (dB/km)	0,2
Comprimento da DCF L_{DCF} (km)	12,8
Dispersão Cromática da DCF D_{DCF} (ps/nm.km)	-100
Inclinação de dispersão (S_{DCF}) da DCF (s/m ³)	-500
Parâmetro não-linear da DCF (m ² /W)	0
Ganho EDFA G_{SMF} (dB)	16
Figura de ruído do EDFA (dB)	4

Fonte: O autor (2020).

2. 3. 4 Receptores

A detecção coerente é um tipo de detecção que, acopla o sinal que está chegando ao receptor ao sinal de um LASER chamado oscilador local (em inglês *local oscillator*, LO). Como resultado desse acoplamento há um deslocamento do sinal, que pode trazer este mesmo sinal para frequências mais baixas. Com isso, o sinal pode

ser movido para banda base ou para uma frequência intermediária. Existem três formas de se fazer a detecção coerente: detecção homódina, heteródina e intradina.

Na detecção homódina, a frequência e a fase do LO precisam ser as mesmas do sinal que está chegando, mas na prática isso é muito difícil de acontecer, devido a duas razões. Primeiro, existe um desvio natural da frequência do LASER, causado por flutuações de temperatura. As variações variam com o tempo, e fazem com que, a frequência do LASER do oscilador local não seja exatamente igual à frequência do sinal que está sendo recebido. A segunda razão é que nenhum LASER é monocromático e é caracterizado por uma certa largura de linha. Essa largura de linha induz a geração de um ruído de fase, que obviamente varia com o tempo. Então, nunca a fase de um LASER vai ser igual à de outro. Por essas duas razões, não é possível a utilização prática deste tipo de detecção em sistemas de comunicações ópticas. O uso desta detecção só seria possível por meio de um controle sobre a frequência de operação do LASER. Este controle teria que compensar a influência de eventuais flutuações de temperatura para que o LASER operasse sempre na mesma frequência.

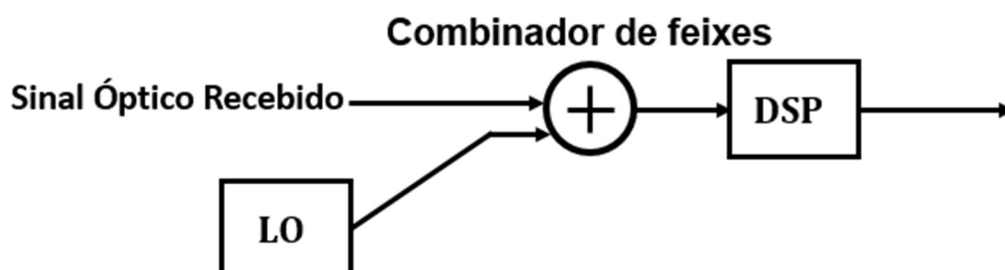
Dado que, a detecção homódina não é prática, uma outra possibilidade seria fazer com que o LO operasse a uma frequência tal do sinal que está chegando que, o batimento entre o LASER do LO e do sinal recebido demodulasse o sinal recebido para uma frequência intermediária na faixa de micro-ondas (AGRAWAL, 2014). O novo sinal em micro-ondas poderia ser assim, demodulado para a banda base. A desvantagem desse tipo de procedimento é a necessidade de um equipamento de micro-ondas, introduzindo um custo adicional ao projeto.

A terceira abordagem é, fazer com que o LO opere em uma frequência de oscilação, que seja a frequência nominal do sinal que está chegando com a informação. Obviamente, as flutuações de temperatura vão causar um desvio relativo de frequência e o ruído de fase vai causar um desvio relativo de fase, entre os dois sinais considerados. Essas flutuações podem ser compensadas no domínio eletrônico, por meio de algoritmos implantados com DSP. Esse terceiro tipo de detecção é chamado de detecção coerente intradina, e é o mais utilizado na prática.

Neste trabalho foi emulado um receptor com detecção coerente homódina. Porém, junto à técnica escolhida, na recepção fez-se o uso de DSP. Empregando-se

um sistema homódino, em que a fase da portadora era estimada no processamento digital do sinal (NETO, 2015), como ilustrado na Figura 10.

Figura 10 – Detecção Coerente Homódina, com utilização de Processamento Digital de Sinais



Fonte: O autor (2020).

Portanto, na recuperação dos sinais já decodificados, os sinais chegam em quatro receptores ópticos distintos. Sendo que, cada sinal foi combinado com o LO, que tinha a mesma frequência de operação e potência original da portadora do sinal. Logo em R_{x_1} e R_{x_3} a frequência de operação do LO é 193,05 THz, e de R_{x_2} e R_{x_4} é 193,15 THz. Em todos os receptores os osciladores tinham a potência de 1,65 mW. Assim, os sinais combinados foram processados digitalmente (BRAGAGNOLLE; NOGUEIRA; SANTOS; PRADO; FERREIRA; FAGOTTO; ALDAYA; ABBADE, 2019) equalizando, corrigindo a dispersão cromática e distorções, para finalmente demodular cada sinal.

3 RESULTADOS

Este Capítulo apresenta os resultados das simulações feitas com a técnica descrita no Capítulo 2. A primeira seção, apresenta os resultados das simulações em que se considera um canal óptico AWGN B2B. Na segunda seção, os resultados referem-se às simulações realizadas com o canal óptico AWGN na TON descrita na Seção 2.3.3.

Os resultados que são apresentados neste capítulo, devem seguir algumas métricas, que garantem o sucesso da aplicação da técnica de criptografia discutida, essas métricas são:

1. O sinal descriptado deve ter uma taxa de erro de bit bem mais baixa, em relação à BER do sinal encriptado, com um valor menor, ou igual, a $2 \cdot 10^{-3}$, pois este sinal deve ser recuperado corretamente a partir do limiar de recuperação da FEC;
2. Para que o sinal não seja interceptado e descriptado por receptores não autorizados, foi arbitrado o valor 100 vezes maior do que o limite da FEC para não ter erro. Portanto a BER do sinal encriptado deve ser maior, ou igual, a $2 \cdot 10^{-1}$.

Durante as simulações, os sinais ópticos foram divididos em diferentes quantidades de fatias espectrais. Os valores utilizados se basearam no padrão de criptografia avançada (do inglês *advanced encryption standard*, AES). Este padrão necessita de um número mínimo de aproximadamente $6 \cdot 10^{76}$ tentativas para quebrar o AES, o que equivale a (NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, 2001). O número de 128 fatias espectrais foi escolhido por ser a metade de fatias espectrais necessárias para utilizar o AES. O próprio número de tentativas do padrão AES, foi utilizado para definir o valor de divisões do sinal óptico em 256 fatias espectrais no SSS. O terceiro número de fatias escolhido é o de 330, esta escolha se deve a dois fatores, em que o primeiro é a possibilidade do invasor conseguir recuperar 13 fatias espectrais, resultando em 317 fatias válidas (ABBADÉ; BOBADILLA; DE CARVALHO; FERREIRA; BONANI; ALDAYA, 2019). O segundo fator envolve o fator de decaimento, em que as fatias espectrais presentes na região de decaimento têm amplitudes menores que as demais, fazendo essas fatias não possam conter muita informação. O fator de decaimento reduz o número de fatias

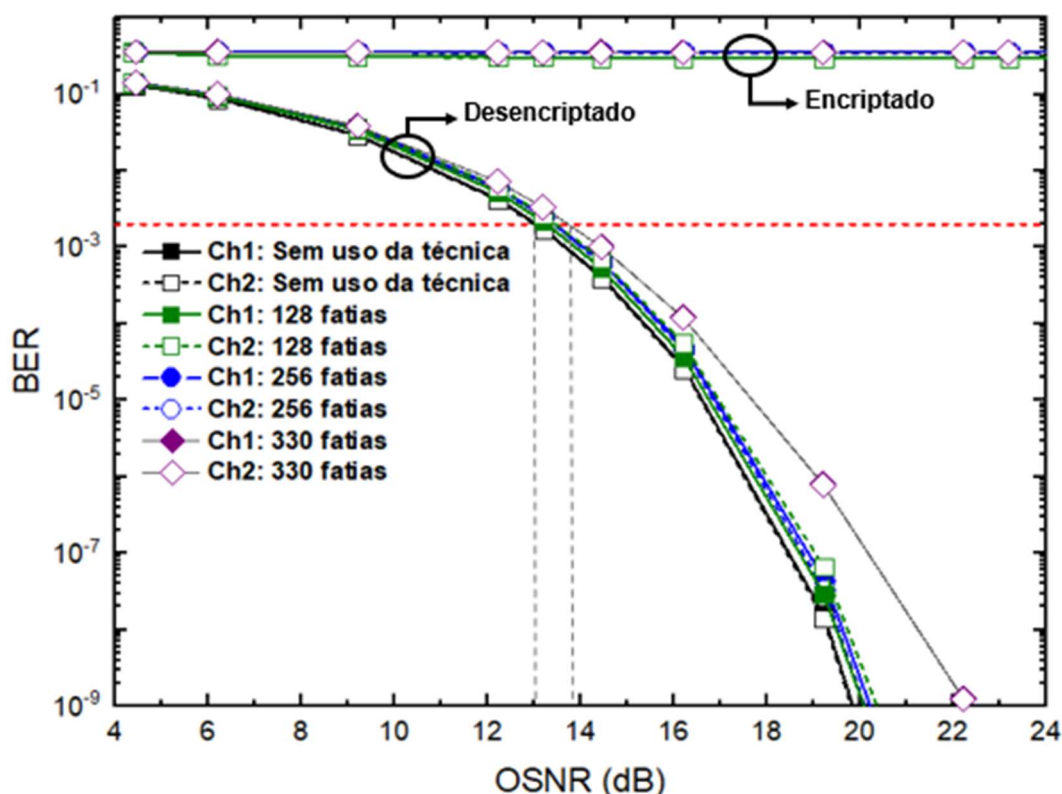
espectrais válidas de 317 para 256 (ABBADÉ; BOBADILLA; DE CARVALHO; FERREIRA; BONANI; ALDAYA, 2019).

Aplicando a Eq. (3) com o número de fatias espectrais de 256 e o erro máximo permitido para que um invasor acerte a fase de uma fatia espectral de 33° (SANTOS, 2020), temos o número mínimo de tentativas estimadas em $2,164 \cdot 10^{103}$. Este valor estimado ultrapassa em 26 casas decimais o valor mínimo da AES.

3. 1 Análise dos Resultados para o Canal AWGN B2B

Por meio das simulações, realizadas com o arranjo configurado em B2B, foi possível analisar sua eficiência quanto à influência do AWGN. Os dados destas simulações, foram utilizados para gerar um gráfico dos resultados da BER em função da razão sinal ruído óptica (do inglês *optical signal-to-noise ratio*, OSNR). Os resultados foram obtidos pelas simulações sem criptografia, portanto, não havendo fatias encriptadas, e também com a criptografia da técnica descrita, aplicada em simulações com 128, 256 e 330 fatias encriptadas.

Figura 11 – Gráfico da BER em função da OSNR para um canal AWGN B2B, sem uso da técnica de criptografia, 128, 256 e 330 fatias encriptadas



Fonte: O autor (2020).

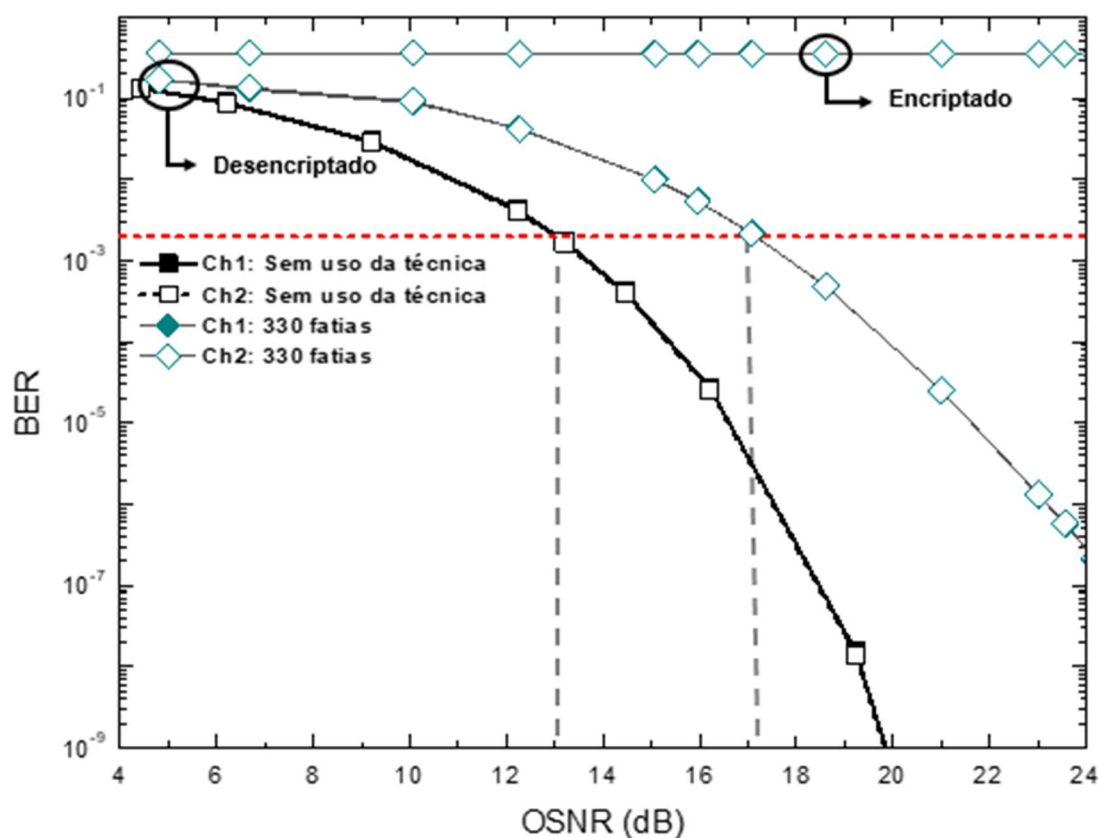
A partir do gráfico ilustrado na Figura 11, é possível afirmar que em um arranjo B2B, a técnica obteve sucesso na criptografia, pois, em qualquer valor da OSNR, a taxa de erro de bit dos sinais encriptados foi maior que o limite máximo de recuperação dos sinais pela FEC, representado pela linha tracejada em vermelho. A BER dos sinais encriptados também esteve acima do limiar estipulado de $2 \cdot 10^{-1}$, garantindo uma maior confiança e a não recuperação da informação por meio de um invasor. A recuperação dos sinais desencriptados, acima de uma OSNR de 13 dB, é possível mesmo sem o uso de FEC. Por meio das linhas tracejadas em cinza, é possível observar que, a variação da OSNR mínima de recuperação de todas as curvas do gráfico, no limiar da FEC, é de aproximadamente 1 dB. Esta variação da OSNR mínima de recuperação, demonstra a robustez da técnica em um arranjo B2B. Nota-se um leve aumento do nível da OSNR mínima de recuperação, quando o sinal óptico é dividido em 330 fatias espectrais na encriptação. Uma explicação plausível para este fenômeno pode ser a sobreposição de algumas das fatias espectrais, ocasionando um efeito degradante ao sinal. Esta interferência deve-se ao alto número de fatias espectrais presentes na simulação, caracterizando diafonia entre as fatias do próprio canal.

3. 2 Análise dos Resultados para o Canal AWGN com 400 km de Propagação

Nesta seção as simulações foram repetidas, porém, os transmissores e receptores estão conectados por meio de uma TON de 400 km de fibra. Esta TON, citada na Seção 2.3.3, utiliza-se de dois caminhos de 400 km cada. Em cada percurso apenas um canal se propaga, evitando diafonia entre esses canais.

O gráfico ilustrado na Figura 12 apresenta simulações somente com 330 fatias espectrais. Pois, este número de fatias já seria capaz de comprovar a eficácia da técnica. Eficácia comprovada ao apresentar um comportamento, relativamente, similar ao gráfico da Figura 11, em que a BER do sinal encriptado está acima de $2 \cdot 10^{-1}$ e também do limiar da FEC, impossibilitando a descriptografia.

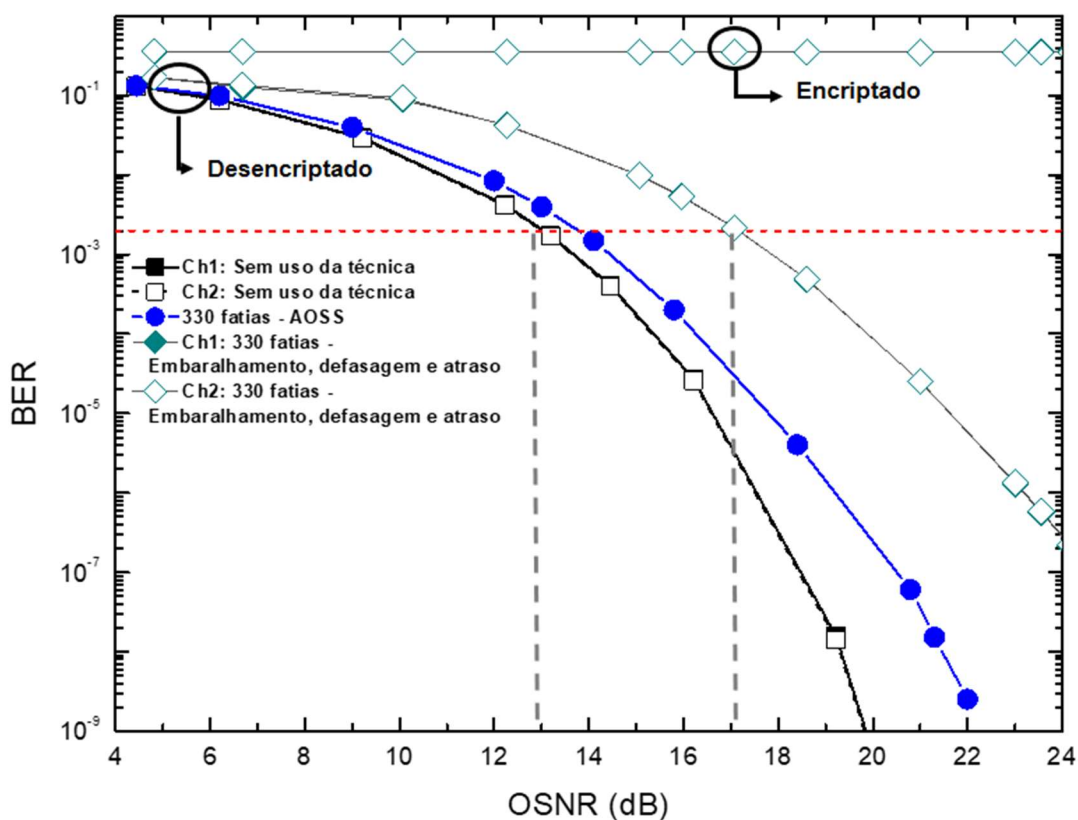
Figura 12 – Gráfico da BER em função da OSNR para um canal AWGN com 400 km de propagação, sem uso da técnica de criptografia e 330 fatias encriptadas



Fonte: O autor (2020).

A OSNR mínima de recuperação com o uso da TON, quando não se faz o uso da técnica é de 13 dB. Quando utiliza-se a técnica com 330 fatias, a recuperação é de aproximadamente 17 dB. O gráfico caracteriza uma penalidade de aproximadamente 4 dB entre a OSNR de recuperação mínima do sinal sem usar a técnica, com o sinal em 330 fatias. Diferente do arranjo configurado em B2B, em que os transmissores estavam conectados diretamente aos receptores, o sinal presente no arranjo desta seção necessita de amplificação óptica para sair do transmissor e chegar ao receptor. A amplificação é realizada por meio dos EDFA, porém, eles injetam o ruído ASE no sistema, o que acarreta uma penalidade maior no momento da detecção do sinal. Outro fator que pode influenciar na penalidade do sinal, é a possível diafonia entre algumas das 330 fatias espectrais.

Figura 13 – Gráfico da BER em função da OSNR para um canal AWGN com 400 km de propagação, sem uso da técnica de criptografia e 330 fatias encriptadas, comparado à técnica AOSS



Fonte: O autor (2020).

Por meio da Figura 13, é ilustrado um gráfico que compara uma técnica de criptografia, em que há somente o embaralhamento das fatias espectrais, codificação óptica por meio de AOSS (BOBADILLA, 2018; ABBADE; BOBADILLA; DE CARVALHO; FERREIRA; BONANI; ALDAYA, 2019). A técnica de criptografia desse trabalho, necessita de uma OSNR mínima na recepção de aproximadamente 17 dB, e a AOSS de uma OSNR mínima de aproximadamente 13,5 dB. Portanto, a implementação de defasagem e atraso nas fatias espectrais para encriptar o sinal, resulta em uma penalidade na OSNR mínima de recepção de aproximadamente 3,5 dB. As informações obtidas no gráfico sugerem que, o grau de complexidade da técnica de encriptação influencia no nível da OSNR mínima, necessária para recuperação do sinal no receptor.

3. 3 Comparação dos Dados das Simulações

Nesta seção os dados apresentados nos gráficos das Figuras 11 e 12 são comparados. É notável a não alteração no valor mínimo da OSNR de recuperação do sinal sem o uso da criptografia, tanto em B2B quanto na TON. O uso da TON não interfere na OSNR do sinal sem criptografia, pois a rede transparente não ocasiona degradação no sinal a ser propagado. Logo, um sinal óptico sem o uso da técnica de criptografia, não apresenta as fatias espectrais que podem realizar uma sobreposição entre outras fatias e deteriorar a OSNR. Deterioração que já é perceptível ao aplicar a técnica no arranjo em B2B, com a penalização de 1 dB, e no arranjo da TON, penalizada em 4 dB. Porém, essa penalidade é o custo de uma maior segurança e complexidade na rede. Na Tabela 4 é possível ver os valores de OSNR mínima necessários para recuperação dos sinais ópticos discutidos.

Tabela 4 – Comparação de OSNR mínima de recuperação

	Sem Criptografia (dB)	Com Criptografia (dB)
B2B	13,0	14,0
TON	13,0	17,0

Fonte: O autor (2020).

Na Tabela 5 é apresentada a comparação entre as OSNRs mínimas de recuperação de cada um dos dados da Tabela 4, assim, confrontada a penalidade de cada aplicação.

Tabela 5 – Penalidade confrontada de OSNR mínima de recuperação

	Penalidade (dB)
Sem Criptografia B2B X Com Criptografia B2B	1,0
Sem Criptografia TON X Com Criptografia TON	4,0
Com Criptografia B2B X Com Criptografia TON	3,0

Fonte: O autor (2020).

4 CONCLUSÕES

Este trabalho consistiu na abordagem referente a análise da técnica de encriptação de sinais ópticos por meio de embaralhamento, defasagem e atraso de fatias espectrais, aplicada em diferentes cenários de uma rede óptica. Essa análise permitiu comprovar o funcionamento da técnica e também entender as dificuldades de sua implementação.

Os resultados obtidos, por meio das simulações da técnica, para a configuração em B2B e para a configuração com a TON de 400 km de fibra óptica, mostram o funcionamento bem-sucedido da técnica com valores de OSNR mínima de recuperação maiores que 14 dB e 17 dB, respectivamente. Em ambos os casos sempre foi alcançada a condição mínima de que a BER do sinal encriptado fosse alta o suficiente para que o invasor não conseguisse interceptar a informação, mesmo com o uso da FEC, e a BER do sinal desencriptado alta o suficiente para poder ser recuperada corretamente por meio de FEC.

A técnica em questão também foi comparada com outra técnica de criptografia óptica, a AOSS. Esta comparação permitiu observar uma relação entre a complexidade da técnica criptográfica e a OSNR mínima de recuperação do sinal óptico. O aumento do grau de complexidade da técnica eleva a OSNR mínima de recuperação, da mesma forma que, a diminuição do grau de complexidade da técnica diminui a OSNR mínima necessária.

As simulações da técnica de encriptação deste trabalho apresentaram uma forte robustez à ataques de força bruta, estimando que o invasor realize um mínimo de $2,164 \cdot 10^{103}$ tentativas para recuperar a informação. Porém é possível aumentar ainda mais a robustez da técnica, aplicando a em um número ainda maior de canais.

REFERÊNCIAS

- ABBADE M. L. F.; BOBADILLA L. D. B.; DE CARVALHO D.O.; FERREIRA A. A.; BONANI L. H. e ALDAYA I. **All-Optical Encryption Using Multi-Channel Spectral Shuffling**. IEEE Photonics Technology Letters, vol. 31, no. 1, pp. 98-101, 1 jan. 2019, doi: 10.1109/LPT.2018.2884477.
- ABBADE, Marcelo L. F. et al. **All-optical cryptography of M-QAM formats by using two-dimensional spectrally sliced keys**. Applied Optics, v. 54, n. 14, p.4359-4365, 5 mai. 2015. The Optical Society.
http://dx.doi.org/10.1364/ao.54.004359.
- ABBADE, Marcelo L. F. et al. **Double all-optical encryption of M-QAM signals based on spectrally sliced encoding keys**. 17th International Conference On Transparent Optical Networks (ICTON), Budapest, p. Tu. A1.3.1-Tu. A1.3.4, jul. 2015. IEEE. http://dx.doi.org/10.1109/icton.2015.7193391.
- ABBADE, Marcelo Luís Francisco et al. **All-optical cryptography through spectral amplitude and delay encoding**. Journal of Microwaves, Optoelectronics and Electromagnetic Applications, v. 12, n. 2, p.376-397, dez. 2013. FapUNIFESP (SciELO). http://dx.doi.org/10.1590/s2179-10742013000200011.
- ABBADE, Marcelo Luís Francisco et al. **All-optical phase and delay spectral encoding of signals with advanced modulation formats**. 16th International Conference on Transparent Optical Networks (ICTON), Graz, jul. 2014. IEEE. http://dx.doi.org/10.1109/icton.2014.6876372.
- AGRAWAL, Govind P. **Sistemas de Comunicação por Fibra Óptica**. 4. ed. [S. l.]: Elsevier Editora Ltda., 2014
- BBC. **NSA-GCHQ Snowden leaks: Aglossary of the key terms**. 2014. Disponível em: <https://www.bbc.com/news/technology-25085592>. Acesso em: 10 mai. 2020.
- BOBADILLA, Leonardo Diogo Bueno. **Criptografia óptica mediante fatiamento e embaralhamento espectrais**. 2018. 50 p. TCC (Graduação) - Curso de Engenharia de Telecomunicações, Câmpus Experimental de São João da Boa Vista, Universidade Estadual Paulista, São João da Boa Vista, 2018.
- BRAGAGNOLLE, T. A.; NOGUEIRA M. P.; SANTOS M. O.; PRADO A. J.; FERREIRA A. A.; FAGOTTO E. A. M.; ALDAYA I., ABBADE M. L. F., **All-optical Spectral Shuffling of Signals Traveling through Different Optical Routes**. Universidade Estadual Paulista (Unesp), Pontifícia Universidade Católica de Campinas (PUC-Campinas), 2019.
- DAHAN D. and MAHLAB U., **Security threats and protection procedures for optical networks**, IET Optoelectronics, vol. 11, no. 5, pp. 186-200, out. 2017, doi: 10.1049/iet-opt.2016.0150.
- GARTNER, Inc. Forecast: **Information Security, Worldwide, 2016-2022, 2Q18 Uptade**. 2018. Disponível em: <https://www.gartner.com/en/documents/3883783/forecast-information-security-worldwide-2016-2022-2q18-u>. Acesso em: 04 ago. 2020.
- GOEDGEBUER, J.-p. et al. **Optical communication with synchronized hyperchaos generated electrooptically**. IEEE Journal of Quantum Electronics,

Piscataway, v. 38, n. 9, p.1178-1183, 7 nov. 2002. IEEE.
<http://dx.doi.org/10.1109/jqe.2002.802025>.

IBGE. **População**. 2020. Disponível em:
<https://www.ibge.gov.br/apps/populacao/projecao/>. Acesso em: 06 ago. 2020.

ICTEYE. **Key ICT data and statistics. International Telecommunication Union (ITU)**. 2019. Disponível em: <http://www.itu.int/net4/itu-d/icteye/AdvancedDataSearch.aspx>. Acesso em: 07 mar. 2019.

INFINERA. **ICE6 800G Generation Optical Engine. 2020**. Disponível em:
<https://www.infinera.com/innovation/ICE6-800G-Wavelengths>. Acesso em: 29 abr. 2020.

IQBAL, Zafar; FATHALLAH, Habib; BELHADJ, Nezh. **Optical fiber tapping: Methods and precautions. In: 8th High Capacity Optical Networks and Enabling Technologies (HONET)**, 2011, Riyadh. Wirelles, RoF and Sattelite Communication. Riyadh: IEEE, 2012. p. 164 - 168.

ISO/IEC/IEEE International Standard - Information technology - Telecommunications and information exchange between systems - Local and metropolitan area networks - Specific requirements - **Part 3: Standard for Ethernet AMENDMENT 10: Media access control parameters, physical layers, and management parameters for 200 Gb/s and 400 Gb/s operation**, ISO/IEC/IEEE 8802-3:2017/Amd.10:2019(E), vol., no., pp.1-376, 28 fev. 2019, doi: 10.1109/IEEESTD.2019.8664714.

JIA Z., CHIEN H., ZHANG J., CAI Y. e YU J, **Performance Comparison of Dual-Carrier 400G with 8/16/32-QAM Modulation Formats**. IEEE Photonics Technology Letters, vol. 27, no. 13, pp. 1414-14171, jul., 2015.

KARTALOPOULOS, Stamatios. **Quantum Cryptography for Secure Optical Networks**. IEEE INTERNATIONAL CONFERENCE ON COMMUNICATIONS, 2007, Glasgow. Computer and Communications Network Security Symposium. Glasgow: IEEE, 2007.

KEISER, Gerd. **Comunicações por Fibras Ópticas**. 4. ed. Porto Alegre: AMGH, 2014. 696 p.

KIM J. H, JHON Y. M., Byun Y. T., LEE S., WOO D. H. e KIM S. H., **All-optical XOR gate using semiconductor optical amplifiers without additional input beam**, IEEE Photonics Technology Letters, vol. 14, no. 10, pp. 1436-1438, out. 2002, doi: 10.1109/LPT.2002.801841.

KITAYAMA, Ken-ichi et al. **Security in Photonic Networks: Threats and Security Enhancement**. Journal of Lightwave Technology, Piscataway, v. 29, n. 21, p.3210-3222, 1 nov. 2011. Institute of Electrical and Electronics Engineers (IEEE).
<http://dx.doi.org/10.1109/jlt.2011.2166248>.

KONG M. et al., **WDM Transmission of 600G Carriers Over 5,600 km with Probabilistically Shaped 16QAM at 106 Gbaud**, 2019 Optical Fiber Communications Conference and Exhibition (OFC), San Diego, CA, USA, 2019, pp. 1-3.

KOSTINSKI, N.; KRAVTSOV, K.; PRUCNAL, P. **Demonstration of an All-Optical OCDMA Encryption and Decryption System with Variable Two-Code Keying**. IEEE Photonics Technology Letters, v. 20, n. 24, p.2045-2047, 15 dez. 2008. IEEE.
<http://dx.doi.org/10.1109/lpt.2008.2006063>.

LATHI, B. P.; DING, Zhi. **Sistemas de Comunicações Analógicas e Digitais Modernos**. 4. ed. Rio de Janeiro: LTC, 2012. 862 p.

LYDIA, Bouchoucha; SMAIL, Berrah; MOHAMED, Sellami. **Application of quantum cryptography in an optical link**. INTERNATIONAL CONFERENCE ON ELECTRICAL ENGINEERING, mai. 2017, Boumerdes. Electrical Engineering Conference. Boumerdes: IEEE, 2017.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. **Advanced Encryption Standard (AES) (FIPS PUB 197): Announcing the Advanced Encryption Standard (AES)**. Gaithersburg: Federal Information Processing Standards Publications (FIPS PUBS), 2001. Disponível em: <<https://dx.doi.org/10.6028/NIST.FIPS.197>>. Acesso em: 19 jul. 2020.

NETO, O. A. L., **Caracterização Sistêmica de um Transmissor Integrado DP-QPSK**. Orientador: Mônica de Lacerda Rocha. 2015. Trabalho de Conclusão de Curso (Bacharelado em Engenharia de Computação) - Universidade de São Paulo, São Carlos, 2014.

PONEMON INSTITUTE/IBM SECURITY. **Cost of a Data Breach Report – 2019**. 2018.

RAMASWAMI, Rajiv; SIVARAJAN, Kumar; SASAKI, Galen. **Optical Networks: A Practical Perspective**. 3. ed. Burlington: Elsevier, 2009. 928 p

SANTOS, Melissa de Oliveira. **Criptografia na Camada Física Baseada em Codificação Espectral Implantada por Meio de DSP e Aplicada a Redes Ópticas**. 2020. 66 f. Dissertação (Mestrado) - Curso de Engenharia Elétrica, Universidade Estadual Paulista, São João da Boa Vista, 2020.

SINGH, S. **O Livro dos Códigos**. 11. ed. [S. l.]: Record, 2001.

SOTO H., ERASME D. and GUEKOS G., 5-Gb/s XOR optical gate based on cross-polarization modulation in semiconductor optical amplifiers. IEEE Photonics Technology Letters, vol. 13, no. 4, pp. 335-337, abr. 2001, doi: 10.1109/68.917843.

TANENBAUM, A. S. **Redes de Computadores**. 5ª Ed., Pearson. 2011.

THE GUARDIAN. **GCHQ taps fibre-optic cables for secret access to world's communications**. 2013. Disponível em: <<https://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa>>. Acesso em 10 mai. 2020.

WANG, Xu et al. **OCDMA over WDM Transmission**. 2007 9th International Conference on Transparent Optical Networks, Roma, jul. 2007. IEEE. <http://dx.doi.org/10.1109/icton.2007.4296043>.

WANG, Xu; WADA, Naoya. **Spectral phase encoding of ultra-short optical pulse in time domain for OCDMA** application. Optics Express, v. 15, n. 12, p.7319-7326, 2007. The Optical Society. <http://dx.doi.org/10.1364/oe.15.007319>.

ZHANG M., CUI Y., ZHAN Y., ZHANG Z. e CHEN X. **Optical encryption/decryption of 8PSK signal using FWM-based modified XOR**, Appl. Opt. 54, 7813-7819 (2015)