UNIVERSIDADE ESTADUAL PAULISTA
"JÚLIO DE MESQUITA FILHO"
Instituto de Ciência e Tecnologia de Sorocaba
Campus de São João da boa vista

MARCELO PEREIRA NOGUEIRA

Criptografia de Sinais por Codificação Espectral de Fase e Embaralhamento Espectral de Amostras em Redes Ópticas Transparentes

São João da Boa Vista
2025

MARCELO PEREIRA NOGUEIRA

Criptografia de Sinais por Codificação Espectral de Fase e Embaralhamento Espectral de Amostras em Redes Ópticas Transparentes

Dissertação apresentada à Universidade Estadual Júlio de Mesquita Filho – Câmpus de São João da Boa Vista para obtenção do título de Mestre em Engenharia Elétrica pelo Programa de Pós-graduação em Engenharia Elétrica.

Área de concentração: Automação e Sistemas Eletrônicos

Orientador: Prof. Dr. Marcelo Luís Francisco Abbade

São João da Boa Vista

2025

N778c

Nogueira, Marcelo Pereira
Criptografia de Sinais por Codificação Espectral de Fase e Embaralhamento Espectral de Amostras em Redes Ópticas Transparentes / Marcelo Pereira Nogueira. -- São João da Boa Vista, 2025
99 p.

Dissertação (mestrado) - Universidade Estadual Paulista (UNESP), Faculdade de Engenharia, São João da Boa Vista
Orientadora: Marcelo Luís Francisco Abbade
Coorientadora: Ivan Aritz Aldaya Garde

1. Criptografia. 2. Sistemas de telecomunicação. 3. Comunicações ópticas. 4. Proteção de dados. 5. Segurança de sistemas. I. Título.

Sistema de geração automática de fichas catalográficas da Unesp. Dados fornecidos pelo autor(a).

Impacto potencial desta pesquisa

Avaliam-se técnicas para criptografar sinais e evitar espionagem em redes ópticas. A proposta é economicamente viável para sistemas que empreguem processamento digital de sinal e, socialmente, fortalece a privacidade de informações sensíveis. As técnicas pesquisadas podem ser estendidas a outros cenários como hospitalares, industriais e militares.

Potential impact of this research

Techniques for encrypting signals and preventing espionage in optical networks are evaluated. The proposal is economically viable for systems employing digital signal processing and, socially, strengthens the privacy of sensitive information. The researched techniques can be extended to other scenarios such as healthcare, industrial, and military applications.

CERTIFICADO DE APROVAÇÃO

TÍTULO DA DISSERTAÇÃO: Criptografia de Sinais por Codificação Espectral de Fase e Embaralhamento Espectral de Amostras em Redes Ópticas Transparentes

AUTOR: MARCELO PEREIRA NOGUEIRA

ORIENTADOR: MARCELO LUÍS FRANCISCO ABBADE

Aprovado como parte das exigências para obtenção do Título de Mestre em Engenharia Elétrica, área: Sistemas Eletrônicos pela Comissão Examinadora:

Prof. Dr. MARCELO LUÍS FRANCISCO ABBADE (Participaçao Virtual)
Departamento de Engenharia Eletronica e de Telecomunicacoes / Faculdade de Engenharia de Sao Joao da Boa Vista UNESP

Prof. Dr. IGUATEMI EDUARDO DA FONSECA (Participaçao Virtual)
Departamento de Sistemas de Computação / Universidade Federal da Paraíba

Prof. Dr. RAFAEL ABRANTES PENCHEL (Participaçao Virtual)
Departamento de Engenharia Eletronica e de Telecomunicacoes / Faculdade de Engenharia de Sao Joao da Boa Vista UNESP

São João da Boa Vista, 29 de novembro de 2024

Verônica Liberali Messias
Supervisora Técnica de Seção
Seção Técnica de Graduação e Pós-Graduação

Assinado de forma digital por Veronica Liberali Messias:36823715839
Dados: 2024.12.13 13:43:04 -03'00'

"Dedico este trabalho à Deus, aos meus pais, ao meu irmão e a todos os amigos e colegas de trabalho que, com amor e apoio, me incentivaram e motivaram a seguir em frente e não desistir da vida"

AGRADECIMENTOS

Agradeço a Deus primeiramente por sempre me auxiliar em todos as etapas da minha vida e me permitir viver até o presente momento.

Aos meus pais, Marcos Nogueira e Célia Pires Pereira Nogueira, e ao meu irmão, Marcos Pereira Nogueira, por acreditarem em mim e me proporcionarem meios de realizar minhas conquistas pessoais e profissionais.

Ao meu orientador, Marcelo Luís Francisco Abbade, e ao meu coorientador, Ivan Aritz Aldaya Garde, por sempre me receberem bem, pelo compartilhamento de conhecimentos, pela paciência de me ensinarem e ajudarem no meu desenvolvimento pessoal e profissional. Fatores esses que me possibilitaram concluir trabalhos anteriores e, em especial, pela realização deste trabalho de dissertação de mestrado.

Aos meus colegas de trabalho do CPQD, que me incentivaram e me proporcionaram meios de realizar e concluir este trabalho.

Aos meus amigos, professores e funcionários da UNESP, que me incentivaram a não desistir dos meus estudos e, mesmo passando por momentos difíceis, me ajudaram a continuar.

"A ciência será sempre uma busca e jamais uma descoberta. É uma viagem, nunca uma chegada."

(Karl Popper)

RESUMO

A segurança da informação tornou-se um tema de grande importância devido às altas taxas de transmissão e ao crescente número de usuários e dispositivos conectados à Internet. O uso de técnicas de criptografia tem se mostrado uma solução eficaz para dificultar a interceptação e compreensão não autorizada do conteúdo das informações transmitidas. Este trabalho avalia a viabilidade de técnicas de criptografia na camada física, aplicadas a sinais propagados em uma rede óptica transparente (*transparent optical network,* TON), desenvolvida em um ambiente computacional. As técnicas de criptografia avaliadas incluem codificação de fase espectral, embaralhamento espectral intercanais e intracanal, baseados em processamento digital de sinal (spectral phase encoding, spectral shuffling, and scrambling in digital signal processing, SPE-SS-Scr-DSP) com o uso de chaves dinâmicas (*dynamic key*, DK). Estas técnicas foram aplicadas a sinais com dupla polarização, em diferentes taxas de transmissão e sinalizações. A geração, criptografia, descriptografia e recuperação dos sinais foram realizadas no *software* Matlab®, enquanto a TON foi desenvolvida no *software* VPITransmissorMaker™, simulando a propagação de sinais em um sistema de comunicação óptico com detecção coerente. A principal métrica utilizada para avaliar a qualidade do sinal e a viabilidade das técnicas foi o alcance obtido após a propagação do sinal por um determinado comprimento de enlace de fibra óptica, considerando uma taxa de erro de bit (*bit error ratio*, BER) específica. Sinais criptografados transmitidos por uma ou por duas rotas possuíram valores de BER superiores ao limite de correção para frente de erro (*forward error correction*, FEC). No entanto, as técnicas de criptografia empregadas, bem como as melhorias desenvolvidas, não geraram penalidades significativas aos sinais transmitidos e recuperados por uma única rota em comparação com os sinais não criptografados. Já os sinais com modulações distintas transmitidos por duas rotas, sendo uma rota com comprimento de fibra óptica fixo e a outra com comprimento variado, mostraram um alcance maior do que os sinais transmitidos por apenas uma rota. As técnicas desenvolvidas mostraram uma boa viabilidade para aplicações em redes ópticas.

Palavras-chave: Técnicas de criptografia. Camada Física. Rede óptica transparente. Processamento digital de sinais.

ABSTRACT

Information security has become a critical issue due to high transmission rates and the growing number of users and devices connected to the Internet. The use of cryptography techniques has proven to be an effective solution to hinder the unauthorized interception and understanding of the transmitted information content. This study evaluates the feasibility of physical-layer cryptography techniques applied to signals propagating in a transparent optical network (TON) within a simulated environment. The evaluated cryptographic techniques include spectral phase encoding, spectral shuffling, and scrambling, all implemented using digital signal processing (SPE-SS-Scr-DSP) with a dynamic key (DK). These techniques were applied to dual-polarized signals, at different transmission rates and signal formats. The generation, encryption, decryption, and recovery of the signals were performed using Matlab® software, while the TON was developed using VPITransmissorMaker™ software, simulating signal propagation in an optical communication system with coherent detection. The main metric used to assess the signal quality and the feasibility of the proposed techniques was the reach obtained after signal propagation over a given length of optical fiber, considering a specific bit error ratio (BER). Encrypted signals transmitted over one or two routes showed BER values above the forward error correction (FEC) limit. However, the cryptography techniques employed, as well as the improvements made, did not significantly degrade the performance of signals transmitted and recovered over a single route when compared to their unencrypted counterparts. Signals transmitted and recovered with different modulations over dual routes demonstrated greater reach than signals transmitted and recovered through a single route. This better performance is attributed to the fixed length of one path and the variable length of the other, and to the influence of propagating two signals with different modulations. The developed techniques have shown promising potential for application in optical networks.

Keywords: Encryption techniques. Physical layer. Transparent optical network. Digital signal processing.

LISTA DE ILUSTRAÇÕES

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

AES	Padrão de criptografia avançado
AWGN	Ruído aditivo, gaussiano e branco
BER	Taxa de erro de bit
bps	bits por segundo
CD	Dispersão Cromática
CIA	Confidencialidade, integridade e viabilidade
CTR	Modo de Contador
DAC	Conversor digital analógico
dB/km	Decibel por quilômetros
dBm	Decibéis miliwatt
DC	Corrente direta
DCF	Fibra compensadora de dispersão
DES	Padrão de criptografia de dados
DK	Chave dinâmica
DSP	Processamento digital de sinal
EDFA	Amplificador de fibra dopada com érbio
EON	Rede óptica elástica
FEC	Correção posterior de erro
FFT	Transformada rápida de Fourier
Gbaud	Gigabaud
Gbps	Gigabits por segundo
I	Componente em fase do sinal
IBGE	Instituto brasileiro de geografia e estatística

IFFT	Transformada rápida de Fourier inversa
ISI	Interferência intersimbólicas
ITU	União internacional das telecomunicações
kbps	Quilobits por segundo
kHz	Quilohertz
Laser CW	Laser de onda contínua
LO	Oscilador local
Mbps	Megabits por segundo
m^2/W	Metros ao quadrado por Watts
MZM	Modulador Mach-Zehnder
NMS	Sistema de gerenciamento de rede
OFDM	Multiplexação por Divisão de Frequência Ortogonal
OSI	Interconexão de sistemas abertos
OTDR	Refletômetro ótico no domínio do tempo
PAM	Modulação por amplitude de pulso
$pA/Hz^{1/2}$	Picoampère por raiz de Hertz
PBC	Combinador de feixe de polarização
Pbps	Petabits por segundo
PBS	Divisor de feixe de polarização
PCS	Subcamada de codificação física
PD	Fotodetector
PMD	Dispersão dos modos de polarização
PMDS	Subcamada dependente do meio físico
PPA	Algoritmo probabilístico em tempo polinomial

PRBS	Sequência pseudoaleatória de bits
PSGs	Geradores pseudo-aleatórios
ps/nm·km	Picosegundos por nanômetros e quilômetros
Q	Componente em quadratura do sinal
QAM	Modulação de amplitude em quadratura
QKD	Distribuição quântica de chaves
QoS	Qualidade de serviço
QPSK	Modulação por deslocamento de fase em quadratura
RCF	Filtro cosseno-levantado
RX	Receptor
SC	Sinal Criptografado
SCD	Sinal Criptografado e Descriptografado
Scr-DSP	Misturador baseado em DSP ou embaralhamento espectral intracanal baseado em DSP
SCS	Sistemas caóticos sincronizados
SER	Taxa de erros de símbolos
s/√m	Segundos por raiz de metros
SPE-DSP	Codificação espectral de fase baseado em DSP
SPE-SS-DSP	Codificação de fase espectral e embaralhamento espectral intercanal baseado em DSP
SPE-SS-Scr-DSP	Codificação de fase espectral e embaralhamento espectral intercanal e intracanal baseado em DSP
SPM	Automodulação de fase
SSC	Sinal Sem Criptografia
SS-DSP	Embaralhamento espectral baseado em DSP ou embaralhamento espectral

SSMF	Fibra óptica padrão monomodo
Tbps	Terabits por segundo
TEA	Algoritmo de encriptação compacto
TON	Rede óptica transparente
TX	Transmissor
VPI	*VPITransmissorMaker*™
XOR	Ou exclusivo

LISTA DE SÍMBOLOS

%	Percentagem
bit	Digito binário
M	Mensagem de entrada
p_{M_i}	Probabilidade de ocorrência da mensagem de entrada
K	Chave criptográfica
p_{K_i}	Probabilidade associada a chave criptográfica
C	Mensagem criptografada
f_c	Função criptográfica
f_d	Função descriptográfica
$byte$	Conjunto de oito bits
km	quilômetros
nm	nanômetros
$m[n]$	Sinal complexo de entrada no domínio do tempo discretizado
$M[n]$	Sinal complexo de entrada no domínio da frequência discretizada
nch	Número do sinal gerado
n_b	Número de blocos
$d[n]$	Sinal complexo descriptografado no domínio do tempo discretizado
nch_1	Número de sinais gerados com os parâmetros primários
nch_2	Número de sinais gerados com os parâmetros secundários
r	Fator de decaimento do RCF
B_c	Banda codificada do sinal após o RCF
R_{sy}	Taxa de transmissão de símbolos
φ_i	Fase da i-ésima amostra
β_0	Coeficiente linear do alargamento do pulso
$P(C)$	Probabilidade de acerto de símbolos
M_s	Número de símbolos
$P(C\|m_j)$	Probabilidade condicional de acerto de símbolo
$P(m_j)$	Probabilidade de o símbolo ser transmitido

$\boldsymbol{P_{eM}}$	Probabilidade de erro de símbolo
$\boldsymbol{P_{eB}}$	Probabilidade de erro de bit
$\boldsymbol{n_{nch}}$	Número de sinais gerados
$\boldsymbol{K_i}$	Chave inicial
$\boldsymbol{K_t}$	Chave temporária
$\boldsymbol{K_s}$	Chave semente
$\boldsymbol{DK_1}$	Primeiro bloco da chave dinâmica
$\boldsymbol{DK_2}$	Segundo bloco da chave dinâmica
$\boldsymbol{DK_n}$	*n* bloco da chave dinâmica
$\boldsymbol{DK_{n-1}}$	*n* do bloco da chave dinâmica anterior
V	Volts
$\boldsymbol{m}$	Sinal complexo de entrada no domínio do tempo
$\boldsymbol{M}$	Sinal complexo de entrada no domínio da frequência
$\boldsymbol{c}$	Sinal complexo criptografado no domínio do tempo
$\boldsymbol{C}$	Sinal complexo criptografado no domínio da frequência
$\boldsymbol{T}$	Sinal complexo transmitido no domínio da frequência.
$\boldsymbol{d}$	Sinal complexo descriptografado e recuperado no domínio do tempo
$\boldsymbol{D}$	Sinal complexo descriptografado e recuperado no domínio da frequência

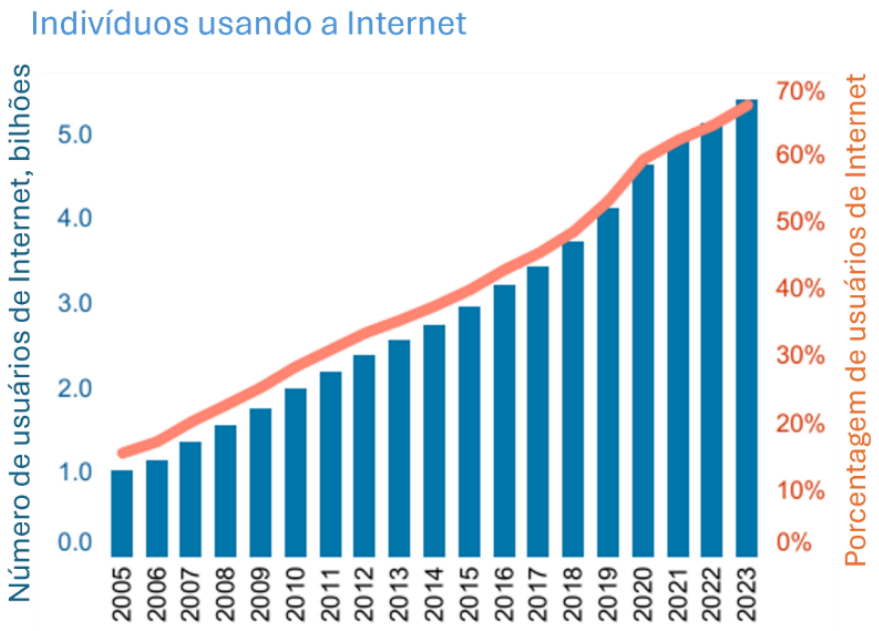
SUMÁRIO

1. INTRODUÇÃO

Nas últimas décadas, o tráfego na Internet e a quantidade de dados utilizados têm crescido significativamente, impulsionado pela crescente demanda por maiores taxas de transmissão e largura de banda (CISCO, 2020), (CISCO VISUAL NETWORKING INDEX, 2017), (GERSTEL, 2012). Esse aumento é consequência do expressivo acréscimo no número de usuários, dispositivos e aplicativos conectados, especialmente com o advento da Internet das Coisas (IoT) (CISCO, 2020). Esse fenômeno requer uma evolução contínua das tecnologias de comunicação e da infraestrutura de redes para atender às exigências emergentes.

O número de usuários de Internet estimado pela União Internacional das Telecomunicações (*International Telecommunication Union*, ITU) em 2023 foi de 5,4 bilhões, representando 67 % da população mundial (ITU, 2023). Na Figura 1, é mostrado um gráfico do número de usuários de Internet ao longo do tempo, cuja tendência sugere um crescimento nos próximos anos. No Brasil, de acordo com o Ministério das Comunicações, 80 % dos domicílios e 149 milhões de pessoas tinham acesso à Internet em 2022 (NÚCLEO DE INFORMAÇÃO E COORDENAÇÃO DO PONTO BR, 2023), o que equivale a aproximadamente 73 % da população (IBGE, 2023).

Figura 1 - Crescimento do número de usuários de Internet ao longo dos anos (2005 – 2023).



Fonte: União Internacional das Telecomunicações, 2023 (figura traduzida para o português).

Essa expansão tem resultado em um aumento significativo no volume de dados sensíveis trafegados pela rede, expondo-os a riscos cada vez maiores de vazamento e acesso não autorizado. No Brasil, por exemplo, 2,8 bilhões de dados sensíveis foram expostos em 2021, colocando o país em primeiro lugar no ranking mundial de vazamento de dados, segundo o "Relatório de Atividade Criminosa Online no Brasil" (ADVISOR, 2022). De acordo com a empresa SurShark (SURFSHARK, 2024), especializada em privacidade, o Brasil ocupou o quinto lugar em 2021 e o décimo segundo lugar no primeiro trimestre de 2022 entre os países com mais episódios de vazamento de dados. Apesar de indícios de melhora a partir de 2022, o Brasil ocupa o sexto lugar em 2024, com aproximadamente 8,74 milhões de dados sensíveis expostos (SURFSHARK, 2024).

Nas comunicações, há um mecanismo de gerenciamento de rede chamado sistema de gerenciamento de rede (*network management system*, NMS), utilizado para gerenciar a rede e garantir uma boa qualidade de serviço (*Quality of Service*, QoS). A QoS está relacionada à capacidade de uma rede de fornecer um nível adequado de serviço aos usuários. Os principais objetivos das redes de comunicação são assegurar que a comunicação ocorra de maneira eficiente, maximizando a taxa de transmissão e a distância alcançada. Atualmente, com o aumento dos vazamentos de informações e a crescente dependência de serviços online, fica evidente a necessidade de implementar mecanismos robustos para garantir a segurança da informação. A segurança das comunicações e o impacto da implementação de mecanismos de proteção na QoS tornaram-se alguns dos principais tópicos de discussão (SIDDIQI e J., 2019) (KIM, 2019).

A segurança da informação baseia-se na tríade de confidencialidade, integridade e disponibilidade (*confidentiality, integrity e availability*, CIA) (STALLINGS, 2014). A confidencialidade envolve dois aspectos principais: a proteção dos dados e privacidade. A proteção dos dados assegura que informações confidenciais não sejam acessíveis ou reveladas a indivíduos não autorizados. Enquanto a privacidade garante que apenas indivíduos autorizados tenham o controle sobre o acesso, armazenamento e modificação das informações.

A integridade assegura que as informações sejam modificadas apenas de maneira autorizada e que não sofram alterações indevidas durante a transmissão. A integridade está relacionada a garantir que os dados não sejam alterados ou corrompidos durante o armazenamento, transmissão e tratamento. Informações podem ser comprometidas por

falhas eletromecânicas, quedas de energia, desastres naturais e erros de leitura de dados em dispositivos. Portanto, a integridade busca minimizar a probabilidade de tais falhas e manter a invariabilidade dos dados (STALLINGS, 2014).

A disponibilidade assegura que os sistemas permaneçam operacionais, permitindo que os serviços estejam acessíveis aos usuários autorizados e que possam acessar às informações sempre que necessário. Além disso, a disponibilidade garante que o acesso à informação seja rápido e confiável. Medidas de segurança e manutenção dos dados devem ser implementadas para que o sistema opere de forma confiável (STALLINGS, 2014).

As técnicas utilizadas para garantir a segurança da comunicação podem ser aplicadas em diversas camadas do modelo de referência para Interconexão de Sistemas Abertos (*Open System Interconnections*, OSI) (IOS, 1984). O modelo OSI é composto por sete camadas, que servem como referência para comunicações em redes: aplicação, apresentação, sessão, transporte, rede, enlace e física (TANENBAUM e WETHERALL, 2010).

Importante notar que a unidade de informação entre as camadas de Enlace e Aplicação é o bit. No entanto, a camada física é subdividida em duas subcamadas, cada uma com sua própria unidade de informação. A subcamada superior, chamada Subcamada de Codificação Física (*Physical Coding Sublayer*, PCS), por exemplo, agrupa bits em símbolos, que podem ser a unidade de informação dessa subcamada. A subcamada inferior, denominada Subcamada Dependente do Meio Físico (*Physical Medium Dependent Sublayer*, PMDS), converte os símbolos da PCS em sinais discretos no tempo, representados por amplitudes e fases. Assim, a unidade de informação da PMDS é composta pelas amplitudes e fases desses sinais.

O objetivo principal deste trabalho é abordar a segurança da camada física das redes. A transmissão de sinais nessa camada, seja por meios confinados, como a fibra óptica, seja por meios não confinados, como o ar, pode estar sujeita a diversos ataques. Esses ataques podem ter diferentes objetivos, como interromper o tráfego de informações da rede, degradar a qualidade da comunicação ou realizar espionagem.

Um exemplo é o corte de cabos de fibra óptica, que interrompe a comunicação entre o transmissor e o receptor. Outro exemplo é o *jamming*, que envolve a emissão intencional de sinais interferentes para obstruir ou degradar a comunicação legítima. Esse

tipo de ataque pode degradar significativamente os sinais, tornando a rede menos confiável (ASSIS e SANTOS, 2011) (PEY, NZE e ALBUQUERQUE, 2022). Além desses, outros ataques à camada física podem incluir a inserção de dispositivos maliciosos.

O intruso pode utilizar dispositivos para espionar as informações transmitidas tanto por meios confinados quanto não confinados. A espionagem em meios não confinados, como as redes sem fio, é mais fácil, pois as informações são propagadas pelo ar e podem ser captadas por dispositivos receptores (ORUMA, 2023). Em contraste, a espionagem em meios confinados, como as redes ópticas consideradas neste trabalho, é mais complexa. Nesse caso, o espião pode empregar métodos intrusivos ou não intrusivos para obter informações propagadas pelas fibras ópticas (PANISSON, VIANNA, *et al.*, 2004) (COLLINS, 2013).

De fato, já existe uma proposta de um NMS para detectar ataques e falhas na camada Física. Essa proposta, apresentada por Furdek (FURDEK; SKORIN-KAPOV, 2012), consiste em agir da seguinte maneira:

1. Detectar o ataque: Identificar se há (i) deterioração da qualidade do sinal, (ii) intrusão na fibra, (iii) perda de serviço ou (iv) qualquer outra consequência direta de um ataque;
2. Localizar o ataque: Identificar o local e a fonte do ataque;
3. Reagir ao ataque: Acionar mecanismos de resposta, isolar o ponto de acesso do atacante e neutralizar os efeitos nocivos na rede.
4. Restaurar as conexões: Reparar as conexões afetadas e retomar as comunicações.

Neste trabalho, em particular, a ênfase é avaliar mecanismos úteis para combater a espionagem de sinais propagados em redes ópticas. Nesse contexto, os dispositivos mais comuns em comunicações ópticas usados para a extração de informações em fibras ópticas são o *splitter* e o grampeador óptico (*optical clip-on coupler*), que operam de maneira intrusiva e não intrusiva, respectivamente.

O *splitter* é um dispositivo intrusivo que, para acessar as informações transmitidas pela fibra óptica, pode causar uma parada momentânea da rede. Além disso, a localização dos *splitters*, quando colocados por invasores, pode ser identificada por Reflectômetros Ópticos no Domínio do Tempo (*Optical Time-Domain Reflectometer*, OTDRs)

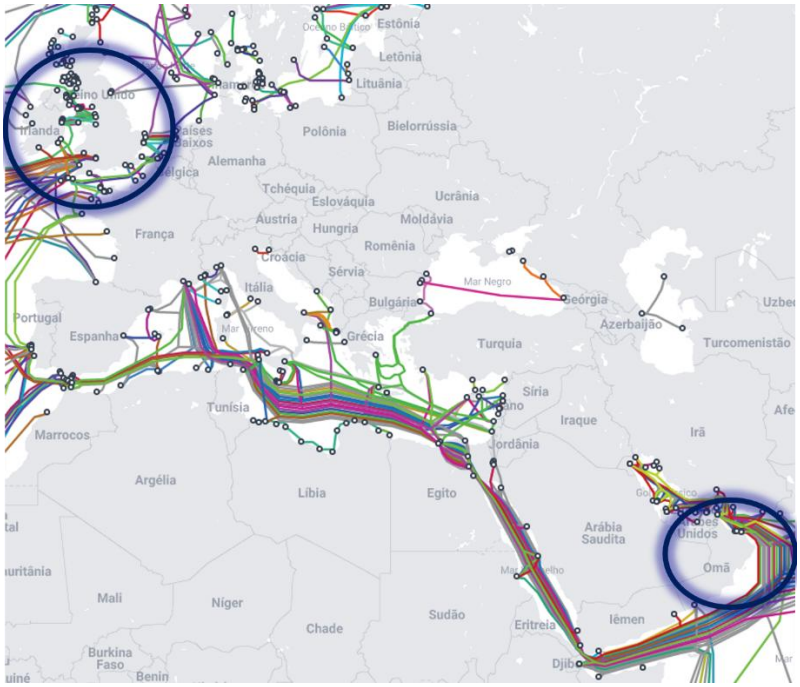
(ABBADE e CAPUTO, 2002) (COLLINS, 2013). Por sua vez, o grampeador óptico é um dispositivo não intrusivo que dobra a fibra óptica, permitindo que parte do sinal escape e se propague externamente à fibra. Esse sinal pode ser amplificado e, então, captado por um receptor óptico. Esse método não causa a interrupção da comunicação na rede e resulta apenas em uma pequena perda de sinal, que pode não ser identificada por OTDRs.

Importante destacar que as informações trafegadas mundialmente utilizam fibras ópticas, interligando continentes e transmitindo dados sensíveis de empresas, países e instituições. Na camada física, as vulnerabilidades são significativas devido à extensão e ao grande número de cabos submarinos transatlânticos que utilizam fibras ópticas para a transmissão de informações. A vasta quantidade e as diversas localizações estratégicas desses cabos tornam a monitoração desafiadora. Muitos desses cabos estão posicionados em locais de importância geopolítica, tornando-os alvos potenciais de ataques por grupos que buscam obter informações de forma ilegal. No entanto, apesar dessas posições estratégicas de monitoração, espiões podem optar por monitorar regiões mais difíceis de serem detectados, como áreas distantes de encostas e localizadas no meio dos oceanos.

Na Figura 2, por exemplo, a costa de Omã é uma região crucial, pois abriga cabos submarinos que conectam a Europa, África, Oriente Médio e Ásia (TELEGEOGRAFY, 2024). Um vazamento de informações nesse ponto pode comprometer a segurança de instituições, empresas e países. Da mesma forma, na Figura 2, pode-se observar que o território do Reino Unido e Irlanda também são estratégicos, pois contém cabos submarinos que ligam a América do Norte, África, Europa, Ásia e a costa de Omã (TELEGEOGRAFY, 2024). Caso espião opte por regiões de mais difícil detecção, existe cabos submarinos no meio de oceanos trafegando informações, que também podem comprometer a segurança. Por exemplo, na Figura 3, são destacadas regiões no meio do Oceano Atlântico Sul onde há cabos submarinos contendo informações correspondentes a comunicação entre os continentes da América do Sul, Europa e a África.

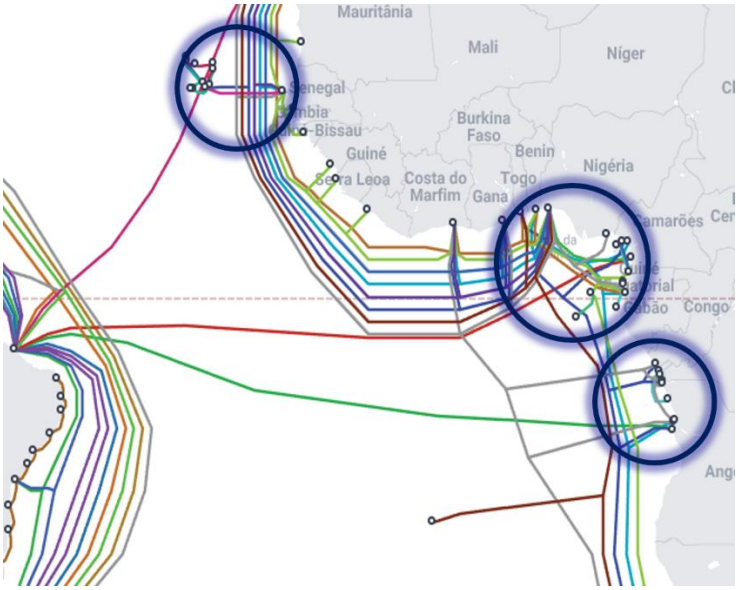
Os pontos estratégicos geopoliticamente, que abrigam a conexão de cabos submarinos ligando diversos continentes, assim como as áreas mais distantes e de difícil detecção, representam ricos significativos para a segurança das informações. Além disso, as três etapas de reação contra ataques e falhas do NMS exigem um tempo e processamento consideráveis. Como mencionado anteriormente, o uso de grampeadores ópticos também dificulta a identificação da espionagem.

Figura 2- Cabos submarinos de fibra óptica interligando Europa, África, Oriente Médio e Ásia destacados na região de Omã e cabos subamarinos de fibra óptica interligando a América do Norte, África, Europa, Ásia e a costa de Omã destacados na região do Reino Unido e Irlanda.



Fonte: *TeleGeografy. Submarine Cable Map*. 2024.

Figura 3- Cabos submarinos de fibra óptica localizados no Oceano Atlântico Sul interligando América do Sul, Europa e a África destacados em diversas regiões de possíveis ataques.



Fonte: *TeleGeografy. Submarine Cable Map*. 2024.

Uma solução possível para mitigar a vulnerabilidade à espionagem é a criptografa da informação. Em sistemas comerciais, as informações já são criptografadas entre as camadas de Enlace e Aplicação. Além disso, soluções proprietárias recentemente desenvolvidas permitem a criptografia de símbolos na PCS. Esses dois tipos de criptografia, destinados à proteção de informações digitais, são referidos neste trabalho como *criptografia de dados*.

Técnicas de criptografia para a PMDS foram relatadas, ao menos, desde 1976 (GALLAGHER, 1976). No entanto, ainda não existe um padrão comercial para a criptografia das unidades de informação dessa subcamada. A criptografia aplicada a essa subcamada é referida neste trabalho como *criptografia de sinais*. O desenvolvimento de técnicas de criptografia de sinais está alinhado com o princípio de que, quanto maior o número de camadas do modelo OSI que realizam criptografia, mais seguras ficam as informações (KITAYAMA, 2011). Conforme detalhado na Seção 1.4, o tema central desta dissertação é a proposta de uma forma de aprimorar e avaliar a técnica de criptografia de sinais baseada no embaralhamento espectral de amostras, proposta por Abbade (ABBADE, NOGUEIRA, *et al.*, 2020) e Nogueira (NOGUEIRA, 2022).

Neste trabalho, parte da criptografia de sinais será baseada em analogias com operações realizadas em criptografia de dados (SOUZA, 2021). Na próxima Seção 1.1, serão abordados aspectos importantes da criptografia de dados, e, na Seção 1.2, serão mencionadas técnicas de criptografia de sinais. Na Seção 1.3, serão apresentadas tecnologias associadas à comunicação óptica, com ênfase em aspectos técnicos e na evolução das redes ópticas. Os objetivos do trabalho estão descritos na Seção 1.4, e a organização do restante da dissertação é detalhada na Seção 1.5.

1.1. Fundamentos da criptografia de dados

As técnicas de criptografia são divididas em dois períodos (KATZ e LINDELL, 2014). O primeiro período corresponde à criptografia clássica, que abrange desde a civilização egípcia, por volta de 1900 a.C., até em torno de 1943 d.C. (DE ARAÚJO, 2018). O segundo período refere-se à criptografia moderna, após o ano de 1943, e vigente até os dias atuais (COZZENS e MILLER, 2013). A criptografia clássica baseava-se principalmente em cifras de substituição e transposição (COZZENS e MILLER, 2013), enquanto a moderna envolve o estudo de técnicas matemáticas para garantir a segurança de informações digitais (KATZ e LINDELL, 2014).

De acordo com Katz (KATZ e LINDELL, 2014), a criptografia moderna também se distingue da criptografia clássica pelos seus usuários e consumidores, que não se limitam mais a organizações militares e governos. Atualmente, a criptografia está presente na vida cotidiana, seja no envio de e-mails, na realização de compras online com cartão de crédito ou no cadastro em aplicativos e sites. A criptografia não é mais utilizada apenas para garantir comunicações secretas com fins militares, mas também se tornou uma ciência essencial para proteger sistemas e informações de pessoas em todo o mundo.

A criptografia moderna tem como base o trabalho seminal de Shannon (SHANNON, 1949), que descreve o desenvolvimento da teoria dos sistemas de sigilo, abordando técnicas, métodos e vulnerabilidades na segurança da informação. A seguir, será apresentado o conceito geral de criptografia moderna. Posteriormente, serão introduzidos dois métodos utilizados na aplicação da criptografia em sistemas de comunicação: a criptografia simétrica e a criptografia assimétrica.

A criptografia é um conjunto de princípios, técnicas e códigos empregados para cifrar informações, tornando-as ininteligíveis para aqueles que não têm autorização de acesso e dificultando que interceptores compreendam o conteúdo das comunicações entre pessoas ou dispositivos. As técnicas de criptografia buscam atingir os objetivos propostos para a segurança dos sistemas de comunicação, sendo fundamentais para garantir a CIA das comunicações (STALLINGS, 2014).

O sistema de comunicação seguro, assim como outros sistemas de comunicação, consiste em três componentes principais: o transmissor, o canal e o receptor. O transmissor é a origem da comunicação, no qual a mensagem é gerada e encriptada. O canal é o conjunto de meios de transmissão e equipamentos que interconectam o transmissor ao receptor. O receptor é o destino, onde a mensagem é recebida, descriptografada e recuperada. O transmissor e o receptor trocam chaves secretas utilizadas para a criptografia e descriptografia da mensagem. A seguir, em linhas gerais, serão descritas as etapas para criptografia e descriptografia de mensagens.

A mensagem enviada pelo transmissor é designada por M e um transmissor pode escolher uma dentre um número finito de possibilidades de mensagens M_i com probabilidade de ocorrência associada a p_{M_i}. Essa mensagem, será encriptada por uma chave criptográfica, K, determinada aleatoriamente com uma probabilidade p_{K_i}. Por

último, a mensagem criptografada é designada por C e está relacionada a M e K (SHANNON, 1949). A fórmula relacionando essas informações é representada por:

$$C = f_c(M, K) \quad (1)$$

Em que C está em função de M e K, e f_c representa uma função de criptografia com duas variáveis.

No receptor, após receber a mensagem criptografada, C, é possível recuperá-la conhecendo C e K pela função f_d, que representa uma função de descriptografia com duas variáveis correspondente a função inversa de f_c. A partir de f_d, obtém a mensagem original M, dada por:

$$M = f_d(C, K) \quad (2)$$

A f_d deve existir exclusivamente para cada C que pode ser obtido a partir de uma mensagem M e uma chave K. Essa formulação base para sistemas seguros foi realizada por Shannon e é descrita com mais detalhes em (SHANNON, 1949). Shannon discute com mais profundidade a criptografia do ponto de vista da teoria da informação e é um dos tratamentos fundamentais da criptografia moderna.

1.1.1. Classificações da criptografia

As técnicas de criptografia são amplamente empregadas para garantir a proteção das informações, e sua classificação é essencial para compreender como podem ser aplicadas. A primeira classificação será em relação as duas categorias utilizadas para operações com chaves, sendo a primeira categoria chamada de criptografia simétrica, enquanto a segunda é chamada de criptografia assimétrica. A segunda classificação será em relação a cifras de fluxo ou de bloco. A seguir, serão explicadas cada uma dessas classificações, destacando as diferentes abordagens de técnicas de criptografia para garantir a segurança da informação.

Na estratégia de criptografia simétrica, o receptor utiliza a mesma chave do transmissor para descriptografar o texto cifrado e recuperar a mensagem original (KATZ e LINDELL, 2014). Essa chave é conhecida apenas pelo transmissor e receptor e é empregada tanto na criptografia quanto na descriptografa da mensagem, sendo conhecida como chave privada. A principal dificuldade nas aplicações de chave privada reside no compartilhamento seguro das chaves (KATZ e LINDELL, 2014).

Em certas situações, as partes envolvidas na comunicação de uma determinada informação podem ter acesso a um canal seguro de comunicação, que utilizam para compartilhar uma chave secreta de forma confiável. Por exemplo, se ambas as partes estiverem próximas em algum momento, podem compartilhar a chave diretamente ou, alternativamente, utilizar um correio confiável (KATZ e LINDELL, 2014). Atualmente, a comunicação quântica está sendo empregada como uma alternativa para o compartilhamento de chaves. Esse método utiliza princípios da mecânica quântica, que se baseiam no comportamento de partículas em nível subatômico, para garantir que qualquer tentativa de interceptação das chaves resulte na alteração da informação. Assim, aumenta-se a segurança do processo (BOARON, BOSO, *et al.*, 2018).

No cenário de criptografia assimétricas, são utilizadas chaves diferentes para criptografar e descriptografar a mensagem. Whitfield Diffie e Martin Hellman introduziram a noção de chaves assimétricas, que consistem em duas partes distintas: uma chave pública e uma chave privada (KATZ e LINDELL, 2014). A chave pública é utilizada para criptografar a mensagem e é amplamente divulgada para múltiplos usuários de uma rede, enquanto a chave privada é utilizada para descriptografar a mensagem e é mantida em segredo pelo emissor e destinatário. O uso dessas duas chaves distintas torna o esquema assimétrico e oferece uma vantagem significativa em termos de segurança.

O protocolo desenvolvido por Diffie e Hellman em 1976, chamado de Diffie-Hellman, revolucionou a criptografia ao introduzir uma nova técnica para a troca de chaves em um canal não seguro, como a comunicação online (KATZ e LINDELL, 2014). O protocolo de Diffie-Hellman é baseado em um problema matemático de difícil resolução, conhecido como logaritmo discreto, o que torna a interceptação das chaves uma tarefa computacionalmente demorada e custosa. Esse protocolo permite que duas partes, em um ambiente público, concordem em uma chave de sessão segura e temporária.

A chave pública, disponível para qualquer pessoa, permite a criptografia de mensagens ou a verificação de assinaturas digitais. Já a chave privada, mantida exclusivamente pelo emissor e pelo destinatário, é a única capaz de descriptografar as mensagens ou assinar digitalmente. No processo de criptografia, uma mensagem criptografada com a chave pública só pode ser descriptografada pela chave privada correspondente, garantindo que apenas o detentor da chave privada tenha acesso ao conteúdo. Já uma mensagem assinada digitalmente com a chave privada pode ser

verificada com a chave pública, assegurando autenticidade e integridade do remetente (KATZ e LINDELL, 2014).

Nesse esquema, o sigilo das mensagens é preservado, mesmo que um invasor conheça a chave pública, pois a chave privada permanece confidencial. O destinatário pode enviar sua chave pública para um remetente potencial ou divulgar a sua chave pública na Internet sem se preocupar com um intruso ou espião. Dessa forma, o esquema de criptografia de chaves públicas permite que exista uma comunicação privada sem depender de um canal privado para distribuição de chaves (KATZ e LINDELL, 2014).

Em resumo, a técnica de criptografia simétrica utiliza chaves idênticas, enquanto a criptografia assimétrica envolve chaves distintas. A criptografia assimétrica exige um processamento computacional mais intenso e é utilizada para que o transmissor e o receptor realizem a troca de chaves de forma segura. Já a criptografia simétrica é mais simples e, portanto, exige menos processamento, possuindo operações que são mais rápidas de serem executadas, sendo utilizada para criptografar a mensagem.

Neste trabalho, utilizou-se a criptografia simétrica pela simplicidade nas operações em comparação com a criptografia assimétrica e pelo enfoque maior na avaliação das técnicas de criptografia e melhorias incorporadas ao código utilizado. Entretanto, a distribuição de chaves utilizando a técnica assimétrica pode ser aplicada a este trabalho em estudos futuros.

A classificação da criptografia de dados pode ser realizada utilizando também o método de cifras de fluxo e de bloco. Na estratégia do método de cifras de fluxo, a mensagem pode ser criptografada bit por bit com um comprimento indefinido. Em contrapartida, o método de cifras de bloco envolve a divisão da mensagem em partes, que são criptografadas em blocos de comprimentos fixos (MENEZES, KATZ, *et al.*, 1996). Embora existam técnicas comerciais que utilizam cifras de fluxo, muitas delas tiveram sua segurança comprometida ao longo do tempo (BARKAN, BIHAM e KELLER, 2003), (LU, MEIER e VAUDENAY, 2005) (WU e PRENEEL, 2006) e (WU e PRENEEL, 2007).

1.1.2. Propriedades da criptografia de dados

As propriedades explicadas a seguir serão em termos da seguridade da técnica empregada, sendo a segurança semântica e a indistinguibilidade de texto cifrado. A segurança semântica é um conceito fundamental na criptografia que garante que um intruso, ao interceptar uma mensagem cifrada gerada por um algoritmo probabilístico em

tempo polinomial (*probabilistic polynomial-time algorithm*, PPA), não consiga extrair informações significativas sobre o conteúdo original da mensagem, exceto dados triviais como o comprimento da mensagem (SHAFI e SILVIO, 1982).

A indistinguibilidade é uma propriedade diretamente relacionada à segurança semântica, e é essencial para garantir que um sistema criptográfico seja considerado seguro (KATZ e LINDELL, 2014). Essa propriedade assegura que um sistema criptográfico torne dois textos cifrados indistinguíveis, mesmo para um observador com conhecimento completo do sistema, exceto pela chave secreta. Dessa forma, um intruso não deve ser capaz de determinar qual das duas mensagens foi encriptada, baseando-se apenas nos textos cifrados resultantes (KATZ e LINDELL, 2014).

Neal Koblitz (KOBLITZ, 1994) estabeleceu uma importante conexão entre a indistinguibilidade e a dificuldade de problemas matemáticos bem estabelecidos. Essa relação demonstra que a segurança criptográfica está profundamente associada à complexidade computacional. Se um adversário fosse capaz de distinguir entre dois textos cifrados, isso implicaria em uma solução eficiente para problemas matemáticos considerados difíceis, como a fatoração de números primos. Isso reforça a importância da indistinguibilidade para garantir a segurança semântica e a robustez de um sistema criptográfico contra diversos tipos de ataques.

Os geradores pseudo-aleatórios (*pseudo-random number generator*, PSGs) desempenham um papel crucial nesse contexto, fornecendo chaves aleatórias e imprevisíveis para os algoritmos de criptografia. A qualidade aleatória dessas chaves é fundamental para garantir a segurança semântica, pois torna mais difícil para um adversário prever o resultado da criptografia e, consequentemente, comprometer a segurança do sistema (SOUZA, 2021).

Neste trabalho, por exemplo, optou-se pela técnica de cifras de bloco. No transmissor, cada bloco da mensagem é criptografado com uma chave específica gerada por um PSG. No receptor, cada bloco é então descriptografado de acordo com a chave correspondente. O uso de chaves geradas a partir de PSGs garante que, ao analisar dois blocos criptografados, um observador não consiga distinguir qual deles corresponde ao bloco original, assegurando, assim, a propriedade de indistinguibilidade.

1.1.3. Principais técnicas de cifras de bloco

As técnicas de cifras de bloco utilizadas em criptografia de dados incluem o padrão de criptografia de dados (*Data Encryption Standard*, DES), o algoritmo de encriptação compacto (*Tiny Encryption Algorithm*, TEA) e o padrão de criptografia avançado (*Advanced Encryption Standard*, AES) (KATZ e LINDELL, 2014). Esses algoritmos de encriptação de dados são baseados em rede de Feistel, que serve como base estrutural para essas técnicas (KATZ e LINDELL, 2014) ou em redes de permutação e substituição (SOUZA, 2021).

A rede de Feistel, segundo Katz (KATZ e LINDELL, 2014), oferece uma maneira de construir uma função irreversível a partir de componentes reversíveis por meio de uma estrutura de repetição em várias iterações. Esse processo garante que, mesmo que as funções envolvidas sejam individualmente reversíveis, o resultado após todas as iterações seja irreversível, a menos que se conheça a chave secreta.

As redes de permutação e substituição realizam operações de substituição de bytes (conjunto de oito bits) na matriz de dados da mensagem e realizam operações de mistura entre as linhas e colunas da matriz, permutando os valores contidos na matriz de dados da mensagem. Embora a grande parte das técnicas de criptografia de dados sejam baseadas na rede de Feistel, a técnica mais utilizada de todas, AES, é baseada em redes de permutação e substituição (SOUZA, 2021).

O AES é um algoritmo de cifras de bloco simétrico, desenvolvido por Vincent Rijmen e Joan Daemen (RIJMEN e DAEMEN, 2001). O algoritmo utiliza cifras de bloco e rede de Feistel, realizando múltiplas iterações para encriptar blocos de 128 bits, utilizando chaves com comprimentos de 128, 192 e 256 bits. Dependendo do comprimento da chave, são designados padrões de referências estabelecidos, sendo AES-128, AES-192 e AES-256.

O AES realiza operações consecutivas de XOR, substituição e permutação. As propriedades de difusão e confusão são garantidas de acordo com o número de iterações realizadas, que varia com o tamanho da chave criptográfica. A propriedade de confusão relaciona o algoritmo de criptografia à chave, que deve ser complexa o suficiente para que a influência de cada bit da chave se espalhe em vários bits da mensagem cifrada (SHANNON, 1949). A confusão é assegurada pela operação de substituição de bytes na matriz de dados da mensagem.

A difusão estabelece que a influência de um bit da mensagem original deve se espalhar em vários bits da mensagem cifrada, sendo garantida pela operação de permutação, que mistura as colunas e linhas da matriz de dados da mensagem. As propriedades de confusão e difusão são descritas com mais detalhes, incluindo as operações da AES, em (DAEMEN e RIJMEN, 1999), (FIPS, 2001) e (SOUZA, 2021).

1.2. Criptografia na camada física

A camada física é responsável pelo tratamento digital do sinal, necessário para converter o sinal do meio digital para o meio físico, possibilitando a transmissão das informações. Nessa camada, além do processamento digital de sinal (*digital signal processing*, DSP) usado para a transmissão, o DSP também pode ser utilizado para incorporar técnicas de criptografia, ampliando a segurança das informações transmitidas.

A PCS, subcamada superior da camada física, opera com informações digitais. Nessa subcamada, a criptografia aplicada à mensagem está alinhada com a criptografia de dados e utiliza técnicas de criptografia já implementadas comercialmente (ABBADE, SOUZA, *et al.*, 2024). Por exemplo, a PCS emprega o algoritmo AES com chave de 256 bits para criptografar dados em redes de comunicação óptica. Outra técnica utilizada nessa subcamada é o embaralhamento de símbolos da constelação.

A PMDS, subcamada inferior da camada física, opera com sinais discretos no tempo, representados por amplitudes e fases. Nessa subcamada, é realizada a criptografia de sinais discretos. Estudos estão explorando técnicas de criptografia de sinais nessa subcamada para aplicações em redes comerciais (ABBADE, SOUZA, *et al.*, 2024). Por exemplo, a PMDS pode empregar técnicas de criptografia espectral de amplitude e fase.

Importante mencionar que os sinais criptografados na PMDS devem ser semelhantes ao ruído durante a transmissão e ter uma baixa taxa de erro de bit (*bit error rate*, BER), idealmente próxima de 0,5 (ABBADE, SOUZA, *et al.*, 2024). Dessa forma, interceptadores não autorizados não devem conseguir identificar corretamente as informações presentes nos sinais transmitidos. Normalmente, os receptores autorizados possuem a chave criptográfica para realizar a descriptografia do sinal e obter informações que se aproximem do sinal original, ou seja, buscando a menor BER possível. As aplicações das técnicas de criptografia não devem, em um cenário ideal, prejudicar a qualidade do sinal descriptografado.

As principais técnicas de criptografia na PMDS que serão mencionadas a seguir são a criptografia caótica, quântica e espectral de fase e amplitude. A criptografia de sinais pode ser aplicada em sinais modulados (ARGYRIS, SYVRIDIS, *et al.*, 2005) (KE, YI, *et al.*, 2016), (CORNEJO e TOCNAYE, 2008) (BOBADILLHA, 2018) ou em banda base (ODEN, LAVROV, *et al.*, 2017) (GENG, YANG, *et al.*, 2018) (SULTAN, YANG, *et al.*, 2018) (SANTOS, 2020) (ABBADE, NOGUEIRA, *et al.*, 2020) (NOGUEIRA, BADUE, *et al.*, 2023).

No caso da criptografia de sinais modulados, por exemplo, a técnica de criptografia caótica, na qual a portadora utilizada para modular o sinal é obtida a partir de uma equação envolvendo a teoria do caos (ARGYRIS, SYVRIDIS, *et al.*, 2005) (ZHANG, XIN, *et al.*, 2011) (KE *et al.*, 2016). No entanto, há problemas na sincronização do sinal no receptor, o que dificulta a utilização dessa técnica (COLET e ROY, 1994). Outro exemplo é a técnica de criptografia espectral de fase, proposta inicialmente por Gallagher em 1976 (GALLAGHER, 1976) e avaliada posteriormente por Cornejo em 2008 (CORNEJO e TOCNAYE, 2008).

A criptografia de sinais modulados tem diversas aplicações e estudos que avaliam sua viabilidade em redes de comunicações ópticas. Entretanto, o alto custo de *hardware* desestimula a adoção dessa técnica. Por outro lado, a criptografia de sinais em banda base pode ser realizada por meio de DSP, que oferece maior flexibilidade de implementação em comparação à criptografia de sinais modulados (SULTAN, YANG, *et al.*, 2018) (SANTOS, 2020) (ABBADE, NOGUEIRA, *et al.*, 2020). Assim, neste trabalho, considerou-se apenas essa segunda vertente.

A criptografia de sinais pode ser realizada por uma abordagem quântica ou clássica da física. Na abordagem quântica, destacam-se, por exemplo, os protocolos BB84 e E91 (MARQUEZINO e HELAYEL-NETO, 2003) (CAMARGO, 2017) (FERREIRA, AMARO e PINHEIRO, 2023) (RIGOLIN e RIEZNIK, 2005) (BANDEIRA, 2013). No entanto, ambos os protocolos operam atualmente apenas a taxas relativamente baixas (ZHANG, TAKESUE, *et al.*, 2009), e a implementação de uma rede quântica implica um alto custo (LYDIA, SMAIL e MOHAMED, 2017).

A utilização prática da comunicação quântica está mais reservada para a troca de chaves, conhecida como distribuição quântica de chaves (*quantum key distribution*, QKD) (IDQ REDEFINING SECURITY, 2020). No estudo realizado por Yin (YIN,

2020), foi possível estabelecer comunicação do satélite chinês Micius entre duas cidades a uma distância de 1120 km, sem a necessidade de repetidores, com uma taxa de transmissão de 0,12 bps. Mais recentemente, Chen e Zhang (CHEN, ZHANG e CHEN, 2021) apresentaram resultados de uma rede de comunicação quântica que conecta pontos a uma distância de até 4600 km, transmitindo chaves a uma taxa de 47,8 kbps.

A melhoria na taxa de transmissão e no alcance em comunicação quântica demonstra um avanço contínuo dessa tecnologia. No entanto, para criptografar os sinais e transmiti-los com taxas compatíveis com os sistemas comerciais atuais, é mais conveniente adotar uma abordagem clássica, que foi utilizada neste trabalho. A criptografia de sinais em banda base, utilizando uma abordagem de física clássica, consiste na criptografia da amplitude e da fase dos sinais (ABBADE, SOUZA, *et al.*, 2024).

A criptografia de amplitude e fase dos sinais pode ocorrer tanto no domínio do tempo quanto no domínio da frequência. No domínio do tempo, essa abordagem apresenta menor complexidade e é realizada mais rapidamente, pois não exige a aplicação da transformada rápida de Fourier (*fast Fourier transform*, FFT) ou da transformada inversa de Fourier (*inverse fast Fourier transform*, IFFT). Entretanto, ao realizar a criptografia nesse domínio, ocorre a perda de correlação entre amostras, o que provoca o alargamento da banda do sinal. Isso pode resultar, por exemplo, em distorções que afetam a qualidade do sinal após a passagem por filtros elétricos já inseridos no sistema de comunicação.

A criptografia de amplitude e fase, quando aplicada no domínio da frequência, apresenta maior complexidade e é implementada de forma mais lenta, devido à necessidade de aplicar a FFT e a IFFT. No entanto, essa abordagem não altera a largura de banda do sinal, pois a criptografia é feita diretamente nas componentes espectrais que compõe a banda. Assim, após a passagem do sinal criptografado por filtros já inseridos no sistema de comunicação, não haverá distorção do sinal. Portanto, as técnicas de criptografia de amplitude e fase utilizadas neste trabalho foram realizadas no domínio da frequência (ABBADE, SOUZA, *et al.*, 2024).

A criptografia espectral de fase é realizada de maneira simples, somando a fase de uma chave à fase do sinal. Em contrapartida, a criptografia espectral de amplitude é mais complexa e, dependendo de seu valor, pode ocasionar penalidades ao sinal. Se a criptografia de amplitude resultar em valores de amplitude muito baixos, o sinal pode ser

prejudicado pelo ruído do canal. Por outro lado, se as amplitudes forem muito altas, o sinal pode ser afetado por efeitos não lineares durante a transmissão em uma rede de comunicação (ABBADE, SOUZA, *et al.*, 2024).

Uma alternativa à criptografia de amplitude é o embaralhamento das amostras dos sinais (ABBADE, NOGUEIRA, *et al.*, 2020). Neste trabalho, utilizou-se o embaralhamento entre amostras de um mesmo sinal e de dois ou mais sinais, em conjunto com a criptografia de fase. Neste trabalho, as principais técnicas de criptografia empregadas incluem a codificação espectral de fase com DSP *(spectral phase encoding digital signal processing*, SPE-DSP), embaralhamento espectral intracanal com DSP (*scramble digital signal processing*, Scr-DSP) e embaralhamento espectral intercanal com DSP (*spectral shuffling digital processing*, SS-DSP). Além dessas técnicas, foram utilizadas chaves dinâmicas (*Dynamic Key*, DK) (SOUZA, NOGUEIRA, *et al.*, 2020) e taxas de transmissão distintas (NOGUEIRA, 2022). A seguir, serão apresentados os principais trabalhos que abordaram essas técnicas.

As técnicas SPE-DSP e Scr-DSP foram estudadas no trabalho realizado por Santos (SANTOS, 2020). A técnica SPE-DSP se baseia em segmentar o sinal em n componentes espectrais, sendo n o número de componentes em que o sinal será dividido. Após essa segmentação, introduz-se uma diferença de fase aleatória em cada componente espectral. A chave criptográfica é derivada dessas variações de fase, permitindo a descriptografia do sinal. Já a técnica Scr-DSP também segmenta o sinal em componentes espectrais, mas realiza o embaralhamento entre essas componentes. A chave criptográfica contém as posições alteradas dessas componentes, possibilitando o desembaralhamento e o retorno às suas posições originais.

As técnicas SPE-DSP e Scr-DSP foram avaliadas por meio de simulações no estudo de Santos (SANTOS, 2020). Ambas foram aplicadas a sinais transmitidos por uma rede óptica, e a qualidade desses sinais foi avaliada utilizando a BER em diferentes esquemas de modulação. O melhor desempenho foi obtido com sinais modulados em 16 modulação de amplitude em quadratura (*Quadrature Amplitude Modulation*, QAM), que apresentaram valores de BER semelhantes entre o sinal criptografado e o sinal sem criptografia, indicando uma boa eficácia das técnicas de criptografia. O alcance máximo desses sinais foi de aproximadamente 700 km de comprimento de enlace de fibra óptica, considerando uma rede óptica transparente (*Transparent Optical Networks*, TON).

A técnica de criptografia SS-DSP, aplicado em redes ópticas, foi estudado por Nogueira (NOGUEIRA, 2019) e publicado por Abbade (ABBADE; NOGUEIRA *et al.*, 2020). A técnica baseia-se no embaralhamento das componentes espectrais entre os *n* sinais gerados. O embaralhamento é definido como a troca, ou não, da amostra na posição *i do i-ésima* sinal pela amostra na posição *i* de outro *i-ésima* sinal. As posições das componentes espectrais trocadas e os sinais para os quais serão alocadas estão contidos em uma chave criptográfica. No processo de desembaralhamento, após a transmissão do sinal criptografado, essa chave é utilizada para restaurar as componentes espectrais aos seus respectivos sinais e posições originais.

No trabalho de Nogueira (NOGUEIRA, 2019), foi demonstrado que a simulação da propagação de dois e quatro sinais criptografados por SS-DSP em uma TON, utilizando apenas uma rota, alcançou um comprimento de enlace de fibra óptica de aproximadamente 700 km. Além disso, a aplicação da criptografia aos sinais não resultou em grandes penalidades em termos de BER. Após a descriptografia e recuperação do sinal transmitido, os valores de BER se mantiveram semelhantes entre os sinais criptografados e os não criptografados.

No estudo de Abbade (ABBADE, NOGUEIRA, *et al.*, 2020), foram apresentados resultados de simulação referentes à transmissão de dois sinais criptografados em SS-DSP por duas rotas distintas, com uma taxa de transmissão de 112 Gbps e modulação em 16QAM. Um dos sinais foi transmitido por uma rota fixa de 480 km de enlace de fibra óptica, enquanto o outro foi transmitido por uma rota variável, alcançando uma distância entre 720 km e 800 km. Essa transmissão de sinais por rotas diferentes aumenta a dificuldade para que um intruso obtenha as informações contidas nos sinais. Como as componentes espectrais estão embaralhadas entre os sinais, é necessário possuir todos os sinais para realizar o desembaralhamento espectral.

Nas técnicas de criptografia, é essencial que se forneça segurança semântica, o que é alcançado, na criptografia de dados, por meio de uma estratégia chamada modo de operação (KATZ e LINDELL, 2014) (FAY, 2016). Um dos modos de operação mais utilizados é o Modo de Contador (*Counter Mode*, CTR), que é uma técnica aplicada em criptografia simétrica para garantir a segurança de dados (FAY, 2016). Essa técnica, em resumo, transforma uma cifra de bloco simétrica em fluxo de cifra. Em criptografias de sinais, por outro lado, as estratégias mais simples envolvem trocar a chave criptográfica

a cada bloco de encriptação. Isso pode ser feito utilizando criptografia caótica digital ou DK (SOUZA, 2021).

A técnica de DK foi proposta por Ngo (NGO, 2010) como uma solução para reduzir os riscos de ataques deliberados. As chaves dinâmicas utilizam criptografia simétrica e podem ser aplicadas para melhorar a segurança e o desempenho de sistemas criptográficos. No trabalho de Souza (SOUZA, NOGUEIRA, *et al.*, 2020), foi desenvolvida a incorporação e adaptação da técnica de DK e AES, para aplicação em sinais utilizando codificação de fase espectral, embaralhamento espectral intercanal e intracanal com DSP (*spectral phase encoding, spectral shuffled and scramble digital signal processing*, SPE-SS-Scr-DSP). A adaptação das técnicas DK e AES para sinais tem como objetivo garantir a segurança da informação transmitida, fundamentando-se nas propriedades de confusão e difusão estabelecidas por Shannon.

No trabalho de Nogueira (NOGUEIRA, 2022), além da utilização das técnicas de codificação espectral de fase e embaralhamento espectral intercanal com DSP (*spectral phase encoding and spectral shuffled digital signal processing*, SPE-SS-DSP) e da técnica de DK, foi realizado um aprimoramento para possibilitar a transmissão de dois sinais gerados com diferentes taxas de transmissão e esquemas de sinalização, visando à aplicação em redes ópticas elásticas (*elastic optical network*, EON).

A alocação de uma banda ampla para utilizar o espectro óptico de maneira mais eficiente, com uma grade mais flexível, tem se mostrado vantajosa, segundo Gerstel (GERSTEL, 2012). Um dos requisitos para uma EON é a capacidade de suportar larguras de banda variadas (ZHANG, DE LEENHEER, *et al.*, 2013). No trabalho desenvolvido por Nogueira (NOGUEIRA, 2022), simulações demonstraram que dois sinais gerados com taxas de transmissões distintas e sinalizações diferentes, criptografados com SPE-SS-DSP e transmitidos em um cenário *back-to-back* em banda base, podem ser descriptografados e recuperados com sucesso.

1.3. Comunicação óptica

A avaliação da viabilidade das técnicas de criptografia SPE-SS-Scr-DSP, com a aplicação de DK a sinais gerados com taxas de transmissão e sinalizações diferentes, foi realizada neste trabalho a partir de uma rede óptica. A rede, desenvolvida em um ambiente computacional, simula uma TON, contendo componentes específicos para uma

comunicação óptica com detecção coerente. Diante disso, nesta seção, serão citadas algumas motivações e conceitos para a utilização da comunicação óptica.

A emergência da tecnologia de comunicação óptica começou por volta de 1950 e se estende até os dias atuais. No estudo realizado por Agrawal (AGRAWAL, 2014), é mencionado um aumento exponencial de 10^6 bps-km até próximo de 10^{15} bps-km entre os anos de 1950 e 2000. As duas principais tecnologias desenvolvidas que permitiram que a comunicação óptica alcançasse grandes taxas de transmissões foram a utilização de fibras ópticas com atenuações muito baixas, em torno de 0,2 dB/km, e o emprego de amplificadores de fibra dopada com érbio (*Erbium-doped Fiber Amplifiers*, EDFA).

As comunicações ópticas, atualmente, adotam tecnologias de modulação avançada, correção de erro posterior (*forward error correction*, FEC), sistemas de detecção coerente e algoritmos de inteligência artificial. Um exemplo é o trabalho realizado por Aparecido de Paula (APARECIDO DE PAULA, ALDAYA, *et al.*, 2023), que propõe uma metodologia de projeto baseada em inteligência artificial, especificamente em redes neurais artificiais. Essa metodologia reduz significativamente a complexidade do processo de otimização dos parâmetros de um modulador eletro-óptico.

Essas tecnologias possibilitaram alcançar distâncias ainda maiores. Segundo Soma (SOMA, 2018), em setembro de 2017, foi possível transmitir 10,16 Pbps utilizando fibras multimodo. Na publicação realizada por Wilkinson (WILKINSON, 2021), menciona-se que a capacidade máxima e a taxa de transmissão de dados obtidas foram de 30 Tbps e 700 Gbps, respectivamente.

A quantidade de dados transmitidos está relacionada à largura da banda de transmissão. Quanto maior a largura do espectro, maior a capacidade de transmissão de informações. Nas comunicações ópticas, existem seis faixas de comprimento de onda, que estão na região entre 1260 nm e 1675 nm (PALAIS, 2004). Na Tabela 1, é mostrada a relação entre os nomes das bandas e suas respectivas faixas de comprimento de onda.

A taxa de transmissão de dados também está relacionada à modulação aplicada ao sinal na rede óptica. Dependendo das características e dos requisitos do projeto da rede, é definido a técnica de modulação empregada. Os moduladores eletro-ópticos utilizados em sistemas de comunicação óptica são descritos em detalhes por Agrawal (AGRAWAL, 2014). Nas simulações deste trabalho, foi utilizado o modulador Mach-Zehnder (*Mach-*

Zehnder Modulator, MZM) para a modulação em fase e amplitude dos sinais modulação por deslocamento de fase em quadratura (*Quadrature Phase Shift Keying*, QPSK) e 16QAM.

Tabela 1 - Banda espectrais em comparação com as faixas de comprimento de onda (nm).

Banda	Faixa de Comprimento de Onda (nm)
O	1260 – 1360
E	1360 – 1460
S	1460 – 1530
C	1530 – 1565
L	1565 – 1625
U	1625 – 1675

Fonte: Elaborado pelo autor.

Outro fator que contribui para o aumento das taxas de transmissão de dados é a utilização das diferentes polarizações da luz durante a propagação dos sinais pela fibra óptica. Os sinais modulados e transmitidos possuem polarizações correspondentes à orientação espacial dos vetores do campo elétrico e magnético, podendo ser lineares, circulares ou elípticas (JENKINS e WHITE, 2001). Em fibras ópticas monomodo, por exemplo, a energia do sinal em um determinado comprimento de onda pode ser decomposta em dois modos de polarizações ortogonais, o que aumenta a taxa de transmissão de dados (JENKINS e WHITE, 2001). Essas polarizações, que são ortogonais entre si, são definidas como polarização horizontal e vertical, denominadas neste trabalho como polarização em X e Y, respectivamente.

Ao utilizar sinais com dupla polarização (X e Y), é possível transmitir praticamente o dobro de informações em comparação à transmissão com uma única polarização (JENKINS e WHITE, 2001). No entanto, essa técnica apresenta uma desvantagem: o efeito de dispersão dos modos de polarização (*polarization mode dispersion*, PMD), que ocorre devido à diferença nas velocidades de propagação entre as polarizações. A diferença do tempo de propagação entre os modos de polarização, chamado de atraso diferencial de grupo, pode causar degradações no sinal, como o alargamento do pulso (JUNIOR, 2003). Atualmente, existem métodos para mitigar esse efeito, como a sincronização dos sinais antes e depois da transmissão pela fibra óptica por meio de equipamento específico, além da compensação da PMD através de algoritmos de DSP.

A alocação de espectro para transferência de grandes volumes de dados tem se tornado uma preocupação crescente, à medida que as taxas de transmissão aumentam significativamente. Segundo Gerstel (GERSTEL, 2012), a modulação do tipo ligado-desligado (*on-off*), que era adequada para taxas de até 10 Gbps, evoluiu para esquemas de modulação mais sofisticados, possibilitando alcançar taxas de até 100 Gbps (BOARON, BOSO, *et al.*, 2018).

A utilização mais eficiente do espectro óptico, com uma grade mais flexível, tem se mostrado conveniente para acomodar larguras de banda mais elevadas (GERSTEL, 2012). Essa maior flexibilidade deu origem a um novo paradigma: as redes ópticas elásticas. Segundo Zhang (ZHANG, DE LEENHEER, *et al.*, 2013), para se tornarem redes flexíveis, as EON devem atender a requisitos como: suportar demandas de taxas de transmissão superiores a 400 Gbps por canal, acomodar diferentes larguras de banda e manter um espaçamento mais estreito entre os canais.

A comunicação óptica tem se destacado também como um sistema fundamental para a implementação da comunicação quântica. No estudo realizado por Boaron (BOARON, BOSO, *et al.*, 2018), é mencionado um alcance de 421 km e uma taxa de transmissão de 6,5 bps para a distribuição segura de QKD a 405 km. Mais recentemente, Fang (FANG, ZENG e LIU, 2020) reportou um alcance de 502 km com uma taxa de transmissão de 0,118 bps. Além disso, Chen (CHEN, ZHANG e CHEN, 2021) mencionou a presença de uma rede com mais de 700 conexões QKD em fibras ópticas, cobrindo uma área de 2000 km. Essa rede óptica está integrada à comunicação via satélite, com um alcance final de 4600 km.

1.4. Contribuições do trabalho

O principal objetivo deste trabalho foi desenvolver um sistema de comunicação óptica em um ambiente computacional para avaliar a viabilidade da aplicação das técnicas de criptografia SPE-SS-Scr-DSP com DK, aplicadas a sinais de dupla polarização e com diferentes taxas de transmissão e esquemas de modulação. As principais etapas desenvolvidas neste trabalho foram:

(i) Desenvolvimento de um cenário de simulação de comunicação óptica com detecção coerente no *software* VPITransmissorMaker™, que se comunica com o *software* KryptosSJ, utilizado no estudo de Nogueira (NOGUEIRA, 2022). O KryptosSJ foi desenvolvido no ambiente Matlab® e inclui a

geração de sinais, a aplicação das técnicas de criptografia SPE-SS-DSP com DK e métodos para a transmissão de sinais com diferentes taxas e sinalizações. A rede óptica desenvolvida possibilitou a simulação da transmissão de sinais de dupla polarização, considerando a influência do efeito de PMD.

(ii) Otimização do sistema de comunicação óptica desenvolvido em (i). Os parâmetros otimizados incluíram a potência do sinal, ajustando o intervalo máximo de tensão na entrada do MZM, bem como a potência do sinal na entrada da fibra óptica. Esses ajustes foram importantes para mitigar os efeitos não lineares tanto no MZM quanto da fibra óptica, incluindo os efeitos de PMD.

(iii) Incorporação e adaptação do código KryptoSJ para geração de *n* sinais, possibilitando a aplicação da criptografia SPE-SS-Scr-DSP em conjunto com a técnica de DK, com limite máximo de duas taxas de transmissão distintas para diferentes esquemas de sinalização.

(iv) Avaliação de um sinal de dupla polarização, criptografado com SPE-SS-Scr-DSP e utilizando DK, gerado com diferentes taxas de transmissão para cada polarização. Essa avaliação foi realizada propagando o sinal por uma única rota na TON.

(v) Avaliação de dois sinais de dupla polarização, criptografados com SPE-SS-Scr-DSP e utilizando DK, gerados com diferentes taxas de transmissão e esquemas de sinalização. Neste cenário, os sinais foram propagados por duas rotas distintas na TON.

O autor, por meio deste trabalho, participou e contribuiu para a publicação de dois artigos: um estudo realizado por Nogueira em 2023 (NOGUEIRA, BADUE, *et al.*, 2023) e, neste ano, um estudo realizado por Pereira (PEREIRA, NOGUEIRA, *et al.*, 2024). Ambos os trabalhos foram apresentados na Conferência Internacional de Redes Ópticas Transparentes (ICTON).

1.5. Organização da dissertação

O restante desta dissertação está organizado da seguinte forma: no Capítulo 2, é descrito o método utilizado durante a execução deste trabalho, detalhando a estrutura desenvolvida em ambiente computacional para simular a propagação de sinais com ou sem criptografia por uma TON. No Capítulo 3, é mostrado e discutido os principais

resultados obtidos deste trabalho. Por fim, no Capítulo 4, é concluído o trabalho com considerações pertinentes e importantes ao longo do desenvolvimento deste trabalho.

2. CÓDIGO E REDE ÓPTICA

A organização do código e o cenário de comunicação utilizado para a transmissão dos sinais são descritos neste capítulo. Na Seção 2.1, é descrito o código desenvolvido em Matlab®, chamado de KryptosSJ e, na Seção 2.2, é descrito o desenvolvimento da TON utilizando o *software* VPITransmissorMaker™ (VPI). O código foi explicado em trabalhos anteriores realizados por Nogueira (NOGUEIRA, 2022), Santos (SANTOS, 2020) e Souza (SOUZA, 2021). Entretanto, neste trabalho, foram adicionadas melhorias e adaptações necessárias ao código para suportar a comunicação entre o Matlab® e o VPI.

As duas melhorias introduzidas no código neste trabalho comparando com o código desenvolvido no trabalho anterior de Nogueira (NOGUEIRA, 2022) foram: possibilidade de geração de n sinais criptografados e a integração da técnica de criptografia chamada de embaralhando espectral intracanais. Neste trabalho, o código contém as seguintes técnicas de criptografia: SPE-DSP, SS-DSP e Scr-DSP. Além dessas técnicas, o código também contém a técnica de DK, a possibilidade de gerar sinais com no máximo duas taxas de transmissão diferentes e a possibilidade de gerar sinais com duas sinalizações diferentes (QPSK e 16QAM).

Neste trabalho, foi convencionado que os sinais no domínio do tempo são designados por letras minúsculas e os sinais no domínio da frequência são designados por letras maiúsculas. A letra que corresponde ao sinal é acompanhada de um número referente ao sinal gerado em conjunto com uma letra indicando a polarização correspondente, sendo em X ou Y (JUNIOR, 2003). Por exemplo, $m_{1,X}[n]$ é o primeiro sinal no domínio do tempo discretizado referente a polarização X; $M_{1,X}[n]$ é o primeiro sinal no domínio da frequência discretizada referente a polarização X; $m_{1,Y}[n]$ é o primeiro sinal no domínio do tempo discretizado na polarização Y e $M_{1,Y}[n]$ é o primeiro sinal no domínio da frequência discretizada na polarização Y. De forma similar, os sinais subsequentes, $m_{2,X}[n]$ e $m_{2,Y}[n]$, correspondem ao segundo sinal no domínio do tempo discretizado referente a polarização X e Y, respectivamente e, os sinais $M_{2,X}[n]$ e $M_{2,Y}[n]$ correspondem ao segundo sinal no domínio da frequência discretizada referente a polarização X e Y, respectivamente.

Os sinais $M_{nch,X}[n]$ e $M_{nch,Y}[n]$ são, respectivamente, a FFT dos sinais $m_{nch,X}[n]$ e $m_{nch,Y}[n]$ (LATHI e DING, 2012). Caso necessário, os sinais no domínio da frequência

podem ser passados para o domínio do tempo aplicando a IFFT. Portanto, os sinais $m_{nch,X}[n]$ e $m_{nch,Y}[n]$ podem ser, respectivamente, a IFFT dos sinais $M_{nch,X}[n]$ e $M_{nch,Y}[n]$. No código, os sinais são gerados subsequentemente e, posteriormente, é ordenado e definido qual sinal que será destinado a transmissão na polarização X ou Y.

Neste capítulo, será utilizado o tipo de sinalização e a parte real ou imaginária em conjunto com a letra que representa o sinal, como, por exemplo, $m_{QPSK\_I}[n]$ e $m_{QPSK\_Q}[n]$. O QPSK indica sinalização adotada, I indica a componente em fase do sinal e Q indica a componente em quadratura do sinal. O I e Q correspondem a parte real e a parte imaginária, respectivamente. O subscrito na letra que representa o sinal pode conter, portanto, o número do sinal gerado, a polarização que o sinal será transmitido, sinalização e a parte imaginária ou real.

A descrição das etapas e a organização do código será realizado a partir da Figura 4, que é um diagrama ilustrativo sobre a organização atual do código. A maioria das etapas são mencionadas e discutidas com mais profundidade nos trabalhos de Nogueira (NOGUEIRA, 2019) (NOGUEIRA, 2022), Souza (SOUZA, 2021) e Santos (SANTOS, 2020). As explicações mais detalhadas serão feitas para as atividades realizadas neste trabalho, sendo melhorias acrescentadas ao código e o desenvolvimento do simulador para um cenário de comunicação óptica coerente.

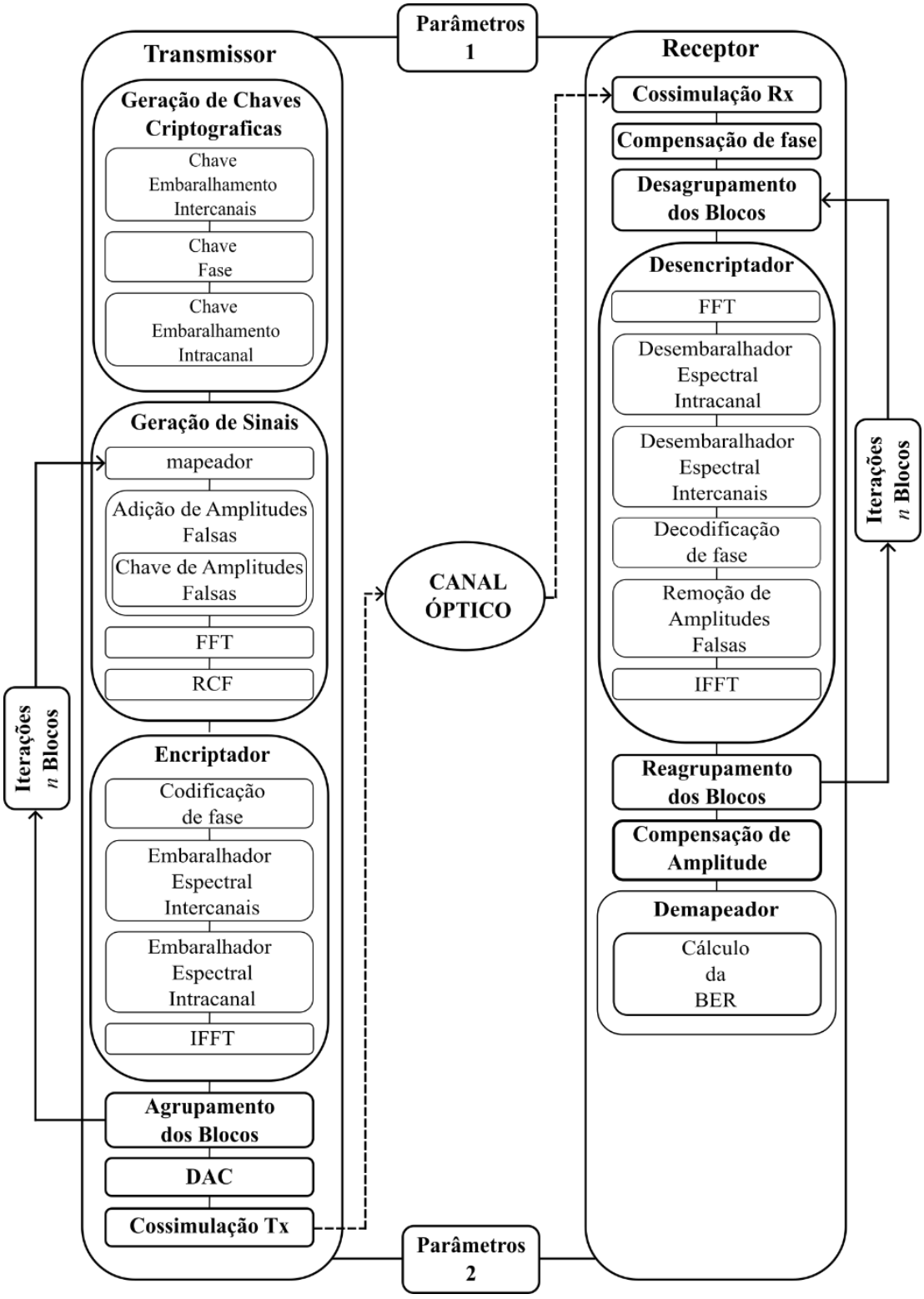
2.1. Organização do código

No diagrama da Figura 4, é representado a organização esquemática do código incluindo todas as melhorias e adaptações realizadas. O diagrama é dividido em 3 módulos, sendo “Transmissor”, “Canal Óptico” e “Receptor”. Os módulos contêm submódulos, sendo “Geração de Chaves Criptográficas”, “Geração de Sinais”, “Encriptador”, “Desencriptador” e “Demapeador”. Nos submódulos contém funções necessárias para a execução do código, como “Mapeador”, “Adição de Amplitudes Falsas”, “FFT”, “IFFT” e “RCF”.

Os submódulos foram classificados como um conjunto de funções, enquanto os módulos foram classificados como um conjunto de submódulos e funções. Os parâmetros utilizados no código estão sendo representado por “Parâmetros 1” e “Parâmetro 2”, nos quais são atribuídos valores para variáveis necessárias e utilizadas ao longo do código. Os parâmetros, como, por exemplo, são o número de amostras, tipo da sinalização, taxa de transmissão e número de símbolos. Há dois arquivos de parâmetros separados para que

as variáveis necessárias para a simulação da transmissão de sinais com taxas e sinalizações diferentes fossem carregadas ao longo do código corretamente. A seguir será explicado os submódulos e as funções do diagrama na ordem de execução do código.

Figura 4 - Diagrama representativo sobre a organização esquemática do código.



Fonte: Elaborado pelo autor.

2.1.1. Transmissor

O módulo “Transmissor” é responsável por gerar, criptografar e transmitir os sinais ao canal. No “Transmissor”, é gerado as chaves criptográficas ou carregado as chaves criptográficas já salvas. A opção de carregar as chaves criptográficas já salvas para diminuir o tempo de simulação é feito atribuindo um determinado valor à variável na função “Parâmetros 1”, sendo o valor de “1” para gerar novamente as chaves criptográficas e “0” para utilizar as chaves criptográficas salvas. Além disso, também é possível atribuir a opção de plotar ou não os gráficos das constelações e dos espectros dos sinais gerados e criptografados.

O submódulo “Geração de Chaves Criptográficas” é responsável pela geração das chaves criptográficas correspondendo as técnicas de criptografia adotadas. No bloco de “Parâmetros 1”, há a opção de escolher qual técnica será utilizada atribuindo o valor de “1” para ativar e o valor de “0” para desativar a técnica de criptografia. No código, há a possibilidade de gerar a chave para a aplicação das criptografias SPE-DSP, SS-DSP e Src-DSP.

As chaves geradas nesse submódulo serão necessárias para criptografar e descriptografar os sinais. As chaves para o embaralhamento intracanal e intercanais contêm as posições que as componentes espectrais serão enviadas e, a chave da codificação de fase contém os valores de fases necessários para deslocar a fase das componentes espectrais do sinal. Nas funções “Chave Embaralhamento Intercanais”, “Chave Embaralhamento Intracanais” e “Chave Fase” são geradas as chaves correspondendo a quantidade de blocos que o sinal irá conter.

A geração de sinais é responsável por gerar os sinais a partir da atribuição dos valores das variáveis definidas nas funções “Parâmetros 1” e “Parâmetros 2”. As variáveis são o número de amostras por símbolo, número de símbolos, número de amostras, sinalização a ser utilizada, banda do sinal, banda codificada do sinal e taxa de transmissão. Os sinais são gerados em cifras de blocos de acordo com o número de blocos (n_b) definido em “Parâmetros 1”. Caso não seja necessário a geração do sinal em diversos blocos, n_b pode assumir valor igual a “1”. Na geração de sinais, possui a opção de gerar sinais com taxas de transmissão diferentes. No caso de gerar sinais com taxas de transmissão diferentes é necessário passar pela função “Adição de Amplitudes Falsas” para igualar a

quantidade de amostras e de símbolos para que a taxa de transmissão de símbolo seja a mesma entre todos os sinais gerados.

Os sinais são gerados na função “Mapeador” a partir de uma sequência pseudoaleatória de bits (*pseudo random bit sequence*, PRBS). Os bits gerados são mapeados em símbolos associados aos eixos I e Q em acordo com o tipo de sinalização definida. Os sinais multiníveis com modulação por amplitude de pulso (*pulse amplitude modulation*, PAM) podem assumir valores de amplitudes diferentes, dependendo do valor de símbolo definido e associados aos eixos I e Q.

Os sinais podem ser gerados como 2PAM ou 4PAM complexos, possuindo valores reais e imaginários. O sinal composto por uma componente real 2PAM e por uma componente imaginária 2PAM será equivalente a sinalização QPSK em banda base. O sinal composto por componentes real 4PAM e por outra componente imaginária 4QAM será equivalente a sinalização 16QAM em banda base.

A sinalização QPSK terá 2 bits por símbolo, já a sinalização 16QAM terá 4 bits por símbolo. Após definido os valores de símbolo e gerado o sinal em bits, são atribuídas as amplitudes ao sinal de acordo com o tipo de sinalização utilizada. Por exemplo, se a sinalização utilizada é QPSK, os valores de amplitude atribuídos serão 1 e -1, enquanto se a sinalização utilizada é 16QAM, os valores de amplitude atribuídos serão -3, -1, 1 e 3.

A quantidade de amostras é ajustada de acordo com o número de amostras por símbolo, por exemplo, no caso de duas amostras por símbolo, a quantidade de amostras é duplicada. Após as atribuições de valores de amplitudes, as palavras geradas para a componente real I e para a componente imaginária Q são associadas e, então, é gerado o sinal complexo $m[n]$. Por exemplo, o sinal gerado com sinalização QPSK, contendo duas amostras por símbolo no domínio do tempo:

m_{QPSK} = [-1-1i 0+0i 1-1i 0+0i -1+1i 0+0i 1+1i 0+0i -1+1i 0+0i -1+1i 0+0i].

Já o sinal gerado com sinalização 16QAM, contendo duas amostras por símbolo:

m_{16QAM} = [1-1i 0+0i -1+3i 0+0i 1+1i 0+0i 1+3i 0+0i 3-3i 0+0i -3 - 3i 0+0i].

A função “Aplicação de Amplitudes Falsas” é utilizada apenas quando há geração de sinais com taxas de transmissão de símbolos e número de símbolos diferentes. Cada

sinal gerado nesse caso possui características particulares (número de amostras, número de símbolos, taxa de transmissão de símbolos e largura de banda). O bloco de “Parâmetros 2” representa a função no código responsável pela declaração das variáveis que serão utilizadas na geração e tratamento dos sinais de modo particular para cada sinal.

Os parâmetros de taxa de transmissão, número de símbolos e número de amostras são definidos no bloco “Parâmetros 2” e podem ser definidos diferentemente para cada sinal gerado. No “Parâmetros 1”, é definido a quantidade de sinais que serão gerados para cada taxa de transmissão e sinalização utilizada. Por exemplo, pode ser definido no código para gerar 3 sinais 16QAM com 56 Gbaud e 2 sinais QPSK com 28 Gbaud. O número máximo que o código suporta atualmente de taxas de transmissão e sinalizações diferentes são duas, sendo possível gerar nch_1 sinais com uma determinada taxa de transmissão e sinalização e nch_2 sinais com outra taxa de transmissão e sinalização.

A técnica de transmissão de sinais com taxas distintas utiliza a adição de amplitudes falsas ao sinal gerado com menor taxa para se igualar ao sinal gerado com maior taxa de transmissão. A adição de amostras falsas remove as diferenças entre os sinais gerados. Nessa função, é gerado a “Chave de Amplitudes Falsas”, contendo os valores das posições correspondentes as amplitudes falsas. A chave é salva e enviada ao receptor em conjunto com as demais chaves para realizar a remoção de amplitudes falsas do sinal. A técnica de adição de amostras falsas aumenta a segurança de dados, pois, mesmo que haja um intruso, não é possível distinguir a diferença entre os sinais transmitidos. No Anexo A, é descrito como é aplicado essa técnica e pode-se encontrar as etapas detalhadas no trabalho desenvolvido em Nogueira (NOGUEIRA, 2022).

A função “FFT” é responsável por passar o sinal do domínio do tempo para o domínio da frequência. O tratamento das componentes espectrais do sinal é mais vantajoso realizar no domínio da frequência, pois se pode alterar as posições das componentes espectral, aplicar um deslocamento de fase e manipular a amplitude do sinal de tal modo a dificultar a desencriptação do sinal transmitido por algum intruso na rede. Além de que, a aplicação do filtro ao sinal é realizada no domínio da frequência. Porém, para a geração, transmissão e análise do sinal é importante obtê-lo no domínio do tempo. A função “IFFT” é a responsável por passar o sinal do domínio da frequência para o domínio do tempo. Ao longo da simulação será, portanto, realizado a transformação do sinal do domínio do tempo para o domínio da frequência e vice-versa quando necessário.

No diagrama da Figura 4, está ilustrado as posições da aplicação das funções da FFT e IFFT ao longo do código. A função “RCF” é responsável por passar o sinal por um filtro de Nyquist com perfil de cosseno levantado (*raised cossine filter*, RCF) para prover a proteção contra interferências intersimbólicas (*intersymbol interference*, ISI) (LATHI e DING, 2012), limitando a banda do sinal por um fator de decaimento (*roll-off*, *r*). A banda do sinal limitada é calculada por

$$B_c = R_{sy}\frac{(1+r)}{2} , \tag{8}$$

Sendo R_{sy} a taxa de transmissão de símbolos do sinal e r o fator de decaimento.

Após o sinal passado pelo RCF é enviado ao módulo “Encriptador”, que contém as funções para aplicação das criptografias. Há três técnicas de criptografias presentes no código, sendo identificadas pelas funções “Codificação de fase”, “Embaralhador Espectral Intercanais” e “Embaralhador Espectral Intracanais” e correspondentes as técnicas de criptografia SPE-DSP, SS-DSP e Scr-DSP, respectivamente.

A função “Codificador de fase” é responsável por aplicar a SPE-DSP ao sinal no domínio da frequência a partir de uma chave, chamada de “Chave de Fase”. Na função “Chave de Fase”, a partir de uma distribuição uniforme, são sorteados valores de fase, φi, que serão utilizados para criptografar as componentes espectrais do sinal (SANTOS, 2020). O conjunto de fase é armazenado em uma matriz, sendo a chave criptográfica de fase. Essa chave é necessária para realizar a codificação de fase do sinal. A codificação de fase é realizada multiplicando as componentes espectrais por $exp(j\varphi_i)$.

A função “Embaralhador Espectral Intercanais” corresponde a técnica SS-DSP (NOGUEIRA, 2019) (ABBADE, NOGUEIRA, *et al.*, 2020). Na técnica SS-DSP, é necessário que, no mínimo, sejam gerados e transmitidos dois sinais. O submódulo “Embaralhamento Espectral” é responsável por aplicar o embaralhamento espectral no domínio da frequência, a partir de uma chave, chamada de “Chave de Embaralhamento”.

No submódulo “Chave de Embaralhamento”, são geradas posições aleatórias para as amostras do sinal e é definido para qual sinal essas amostras serão destinadas. As posições de destino das amostras são armazenadas em uma matriz, que é a chave necessária para realizar o embaralhamento e o desembaralhamento das componentes espectrais dos sinais. O embaralhamento das amostras entre os sinais é realizado trocando as componentes espectrais entre os sinais, com base na chave de embaralhamento.

No caso de utilizar um sinal com duas polarizações, o embaralhamento das componentes espectrais pode ser realizado entre as polarizações (NOGUEIRA, BADUE, *et al.*, 2023). Neste trabalho, os resultados obtidos e mencionados na Seção 3.2, foi utilizado a geração de dois sinais com dupla polarização e o embaralhamento espectral intercanais ocorreu entre as polarizações dos sinais. No Anexo B, está descrito com mais detalhes como é gerado a chave do embaralhamento espectral intercanal e pode-se encontrar em detalhes as operações realizadas no código no trabalho desenvolvido por Nogueira em 2019 (NOGUEIRA, 2019).

A função "Embaralhador Espectral Intracanais" corresponde a técnica Scr-DSP utilizada e explicada no trabalho (SANTOS, 2020). Na técnica de embaralhamento intracanal, diferentemente da técnica de SS-DPS, é realizado o embaralhamento das componentes espectrais do próprio sinal. O submódulo "Embaralhamento Espectral Intracanal" é responsável por aplicar o embaralhamento espectral no domínio da frequência, a partir de uma chave, chamada de "Chave de Embaralhamento Intracanal".

Na função "Chave de Embaralhamento Intracanal", são geradas posições aleatórias para as amostras do sinal, que definem para quais posições essas amostras serão realocadas. As posições de destino das amostras são também armazenadas em uma matriz, sendo a chave de embaralhamento intracanal necessária para realizar o embaralhamento e desembaralhamento das amostras do próprio sinal. O embaralhamento das amostras é realizado trocando as posições das componentes espectrais do sinal com base na chave de embaralhamento intracanal.

Após aplicado as técnicas de criptografias a cada bloco do sinal segmentado, a função "Agrupamento dos Blocos" é responsável por realizar a concatenação dos *n* blocos do sinal no domínio do tempo. A cada iteração é gerado, criptografado e concatenado um determinado bloco do sinal para que ao final de todas as iterações obtenha o sinal completo contendo todos os *n* blocos. Em seguida, o sinal passa pelo conversor digital analógico (*Analog to Digital Conversion*, DAC), que é responsável por realizar a quantização do sinal de acordo com o número de níveis estabelecidos em "Parâmetros 1".

O sinal criptografado, após passado pelo DAC, é, então, enviado para a TON pela função "Cossimulação Tx", que é responsável por estabelecer a comunicação entre o *software* Matlab® e VPI. Nessa função, os sinais criptografados e os parâmetros "*SampleRateDefault*" e "*TimeWindow"* são atribuídos às variáveis contidas em uma

classe já definida e proveniente do VPI. A variável "*SampleRateDefault*" é o valor da taxa de transmissão das amostras e o "*TimeWindow*" é a duração dos sinais que serão analisados no VPI. Os sinais, após a atribuição correta às variáveis, são enviados ao VPI para simulação de transmissão em uma rede óptico (NOGUEIRA, 2019).

2.1.2. Receptor

O módulo "Canal Óptico" foi desenvolvido neste trabalho e corresponde a um ambiente de simulação, onde foi desenvolvido um cenário representando uma TON. Esse módulo, em específico, será descrito e mais detalhado na Seção 2.2.1. Após o sinal passado pela TON, o módulo "Receptor" é responsável por receber e recuperar esses sinais. As funções presentes nesse módulo são responsáveis por realizar o tratamento, descriptografia e compensação necessária para que seja recuperado as informações dos sinais transmitidos.

A função "Cossimulação Rx" é responsável por receber os sinais, provindos do "Canal Óptico", no domínio do tempo por meio da cossimulação estabelecida entre o VPI e Matlab®. O sinal recebido é passado pela função "Compensação de fase", que é responsável por aplicar um valor de fase ao sinal recebido no domínio do tempo para ajustá-lo a posição do estado original. A compensação de fase é necessária, pois o sinal durante a transmissão pela fibra óptica sofre com os efeitos não lineares, como a automodulação de fase (*self-phase modulation*, SPM), e lineares, como a dispersão cromática (*cromatic dispersion*, CD), que resultam na degradação do sinal.

Os efeitos não lineares na fibra óptica em conjunto com a dispersão influenciam na fase do sinal linearmente. O coeficiente linear β_0 do alargamento do pulso, resultante da expansão em uma série de Taylor em torno da frequência central, influência na fase do sinal como descrito no trabalho de Agrawal (AGRAWAL, 2014) e Santos (SANTOS, 2020). Diante dessa penalidade aplicada ao sinal durante a propagação pela fibra óptica, foi necessário aplicar a compensação desse desvio de fase a cada comprimento de fibra óptica simulado.

O sinal recebido e com a fase compensada é, então, enviado a função "Desagrupamento dos Blocos", que é responsável por realizar a separação dos blocos do sinal no domínio do tempo para posterior aplicação das funções responsáveis pela descriptografia e recuperação do sinal transmitido e recebido. O submódulo "Desencriptador" é responsável por realizar a descriptografia e a remoção das amostras

falsas do sinal. A operação de descriptografia e remoção das amostras falsos é realizada por bloco. A cada "iteração *n*" é feita a descriptografia e a recuperação do *n* bloco utilizando a chave criptográfica correspondente (NOGUEIRA, 2022).

A função "Desembaralhador Espectral Intracanais" é responsável por realizar o desembaralhamento das componentes espectrais no domínio da frequência do próprio sinal, a partir da chave de embaralhamento intracanal. As amostras, após aplicada a chave de desembaralhamento espectral ao sinal, são retornadas à sua posição original.

Da mesma forma, a função "Desembaralhador Espectral Intercanais" é responsável por realizar o desembaralhamento das componentes espectrais no domínio da frequência entre os sinais. O desembaralhamento é feito utilizando a chave de embaralhamento intercanais. As amostras, após aplicada essa chave aos sinais, são retornadas ao sinal e à sua posição original.

A função "Decodificação de Fase" é responsável por aplicar a decodificação de fase ao sinal no domínio da frequência. A decodificação é realizada utilizando a chave criptográfica da codificação de fase que é utilizada para desencriptar as componentes espectrais multiplicando-as por $\{exp(j\varphi_i)\}^* = exp(-j\varphi_i)$. Os valores de fase originais são retomados após as componentes espectrais dos sinais serem decodificadas.

A função "Remoção de Amplitudes Falsas" é responsável por remover as amostras falsas acrescentadas ao sinal. As amostras falsas são removidas a partir da chave de amplitude falsas. Após a remoção das amplitudes falsas, o sinal retorna a taxa de transmissão de símbolo, número de símbolo e número de amostras originais (NOGUEIRA, 2022).

A função "Reagrupamento dos Blocos" é responsável por concatenar novamente os blocos do sinal no domínio do tempo. A sua função é semelhante ao "Agrupamento dos Blocos". A cada iteração, é concatenado o bloco do sinal a uma variável até que obtenha o sinal descriptografado por completo.

A função "Compensação de Amplitude" foi desenvolvida no decorrer deste trabalho com objetivo de compensar as variações dos valores de amplitude sofridas durante a transmissão do sinal pela rede óptica. A compensação da amplitude é realizada no domínio do tempo, sendo necessária para que as amplitudes do sinal recebido sejam multiplicadas por uma determinada constante "*k*" e retornem a assumir valores

correspondentes aos valores originais do sinal mapeado e gerado no módulo "Transmissor" de acordo com a sinalização definida.

A seguir, são descritas as etapas realizadas por essa função. O sinal descriptografado, foi nomeado de $d[n]$ e, após o ajuste da amplitude, foi denominado $d'[n]$. As etapas para determinar o valor ótimo da constante para ajustar as amplitudes do sinal são:

1) Separar o sinal recebido em parte real e imaginária, sendo a parte real denominada $d_I[n]$ e a parte imaginária de $d_Q[n]$.
2) Definir um vetor com as amplitudes ideais em acordo com sinalização utilizada e, posteriormente, separá-lo em parte real e imaginária. Por exemplo, no caso de 16QAM:
    a. v_{16QAM} = [-1-1i, -1-3i, -1+1i, -1+3i, -3-1i, -3-3i, -3+1i, -3+3i, 1+1i, 1+3i, 1-1i, 1-3i, 3+1i, 3+3i, 3-1i, 3-3i];
    b. v_{16QAM_I} = [-1,-1,-1,-1,-3,-3,-3,-3, 1, 1, 1, 1, 3, 3, 3, 3];
    c. v_{16QAM_Q} = [-1, -3, 1, 3, -1, -3, 1, 3, 1, 3, -1, -3, 1, 3, -1, -3];
3) Definir um vetor com valores das constantes para multiplicação de $d_I[n]$ e $d_Q[n]$. O vetor, por exemplo, pode variar dentro um determinado intervalo de valores definidos de 0,5 até 10 com passo de 0,01:
    a. v_k = [0,5, 0,51, 0,52, 0,53,..., 9,95, 9,96, 9,97, 9,98, 9,99, 10,00];
    b. O cálculo para descobrir a distância entre as amplitudes do sinal recebido multiplicadas pela constante "k" e as amplitudes ideias dos símbolos é feito utilizando a distância euclidiana. O cálculo no código envolve uma varredura em três níveis. No primeiro nível, um valor da constante "k" é fixado. No segundo nível, um valor de amplitude do sinal recebido é fixado. No terceiro nível, os valores das amplitudes ideais são varridos. A fórmula utilizada para o cálculo da distância entre os valores das amplitudes do sinal multiplicado pela constante "k" e os valores de amplitudes ideais é dada por:

$$D[w] = \sqrt{\left(v_k[i] * d_I[n] - v_{16QAM\_I}[w]\right)^2 + \left(k[i] * d_Q[n] - v_{16QAM\_Q}[w]\right)^2}, \qquad (9)$$

c. Após o cálculo da distância para cada amplitude ideal, o menor valor de distância obtido é selecionado e armazenado em um vetor, nomeado de D_{min}, dado por:

$$D_{min} = \min(D), \tag{10}$$

Na equação (9), "i" é a iteração correspondente ao vetor de constante v_k, "n" a iteração correspondente ao sinal recebido e "w" a iteração correspondente as amplitudes ideias.

O cálculo em (9) e (10) é realizado primeiramente para todos os valores de amplitudes do sinal e para todos os valores dos símbolos ideias. Posteriormente, é calculada a média dos valores de distâncias mínimas e armazenada em um vetor chamado de "D_{mean}":

$$D_{mean}[i] = \frac{\sum_n D_{min}[n]}{n'} \tag{11}$$

Sendo n' o número total de valores contidos no vetor $D_{min}[n]$.

Após o cálculo da média em (11), é variado o valor da constante em v_k e realizado novamente os cálculos em (9), (10) e (11) variando os valores das amplitudes do sinal e dos símbolos ideais e, em seguida, é armazenado a distância média em "D_{mean}". Esse processo é realizado até que todos os valores do vetor de constantes, v_k, sejam varridos. Dessa forma, para cada valor de constante "k", tem-se um valor da distância média mínima calculada.

4) Obter o menor valor da média da distância, ou seja, a distância ótima (D_{opt}), e obter o índice ótimo correspondente a essa menor distância ($ind_{D_{opt}}$):

$$D_{opt}, ind_{D_{opt}} = \min (D_{mean}) \tag{12}$$

5) Obter o valor ótimo da constante, k_{opt}, para ajuste das amplitudes do sinal aplicando o índice ótimo encontrado, $ind_{D_{opt}}$:

$$k_{opt} = v_k \left[ind_{D_{opt}}\right] \tag{13}$$

6) As etapas de 1-5 foram repetidas 5 vezes para que o valor da constante de multiplicação encontrado seja o valor ótimo.
7) Por fim, para ajustar as amplitudes do sinal, multiplica-se as amplitudes do sinal recebido com o valor k_{opt} encontrado:

$$d'[n] = d[n] * k_{opt} \tag{14}$$

Por final, após o sinal ser descriptografado e recuperado, a função “Demapeador” realiza o cálculo para estimar o valor da BER para verificar a qualidade do sinal. A BER é utilizada neste trabalho como métrica de medida para estimar a qualidade do sinal recebido, sendo um valor importante para que seja definido se é ou não possível a recuperação do sinal.

O valor limite da BER adotado, para que seja possível a recuperação do sinal quando aplicado o algoritmo da FEC, é chamado de limite da FEC. Esse valor padronizado da segunda geração pela recomendação da G.975.1 (2004) do ITU-T (TYCHOPOULOS, KOUFOPAYLOU e TOMKOS, 2006) foi considerado de $2 \cdot 10^{-3}$. Os valores de BER considerados livres de erros foram os valores menores que $1 \cdot 10^{-15}$. A constelação do sinal criptografado possui pontos com distribuição aproximadamente gaussiana e a BER do sinal encriptado deve ser maior do que o limite da FEC para que não seja possível a recuperação do sinal, enquanto para o sinal transmitido e descriptografado o valor da BER precisa estar abaixo do limite da FEC.

No submódulo “Demapeador”, é convertido os símbolos recebidos em uma sequência de bits. No cálculo da BER, supõe-se que o sinal transmitido utilizou a codificação de Gray, que impõe a ocorrência de apenas um bit distinto entre símbolos adjacentes e provê uma BER menor do que de outras codificações. Nessa função, a BER é estimada por duas formas descritas a seguir.

Contagem de Erros: A sequência de bits do sinal criptografado e descriptografado são avaliados e se há uma diferença entre os elementos contidos nessas sequências é computado um erro. Porém como mencionado em (SANTOS, 2020) essa técnica apenas pode ser utilizada em condição em que a magnitude da taxa de símbolos de erro (*Symbol Error Rate*, SER) é suficientemente maior que o recíproco do número de símbolos simulados. Se essa condição não for satisfeita, pode resultar em nenhum bit errado detectado ou o número de bits errados detectados pode ser muito baixo e pouco confiável em termos estatísticos. O contador de erros retorna a BER e a SER, que permitem uma comparação qualitativa da qualidade entre os sinais criptografados e descriptografados.

Estimador para distribuição Gaussiana: O estimador retorna a BER e a SER para um receptor de máxima verossimilhança. O cálculo realizado no código foi baseado teoricamente em (LATHI e DING, 2012) e (SANTOS, 2020). A probabilidade de acertos de símbolo é dada por:

$$P(C) = \sum_{j=1}^{M_s} P(C|m_j)P(m_j) \tag{15}$$

Sendo M_s o número de símbolos, $P(C|m_j)$ é a probabilidade condicional de acerto de símbolo dado que o símbolo m_j foi transmitido e $P(m_j)$ é a probabilidade de m_j ser transmitido.

A probabilidade de erro de símbolo é dada pela equação:

$$P_{eM} = 1 - P(C) \tag{16}$$

A aproximação da probabilidade de erro de bit é dada por:

$$P_{eB} = \frac{P_{eM}}{log_2 M_s} \tag{17}$$

As equações da SER para os sinais QPSK e 16QAM em banda-base são dadas por:

$$SER_{QPSK} = erfc\left(\frac{d}{\sqrt{2\sigma_N}}\right) \tag{18}$$

$$SER_{16QAM} = \frac{3}{2} erfc\left(\frac{d}{\sqrt{2\sigma_N}}\right) \tag{19}$$

Sendo $erfc$ a função erro complementar, d a distância de separação entre símbolos adjacentes e σ_N é desvio padrão do ruído do canal. Nas equações (18) e (19), é assumido que durante a propagação do sinal pelo canal foi inserido ruído aditivo, gaussiano e branco (*aditive White Gaussian noise*, AWGN). A BER para esses dois casos é aproximadamente:

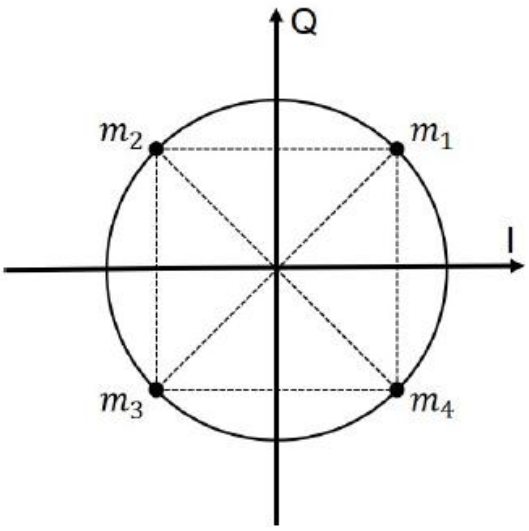
$$BER \approx \frac{SER}{log_2 M} \tag{20}$$

Quando as taxas de erro de bits são suficientemente altas, maiores que $3 \cdot 10^{-3}$, a BER é estimada por contagem de erros, comparando as sequências transmitidas e recebidas de bits. Caso contrário, a estimativa da BER é realizada por distribuição gaussiana.

Na Figura 5, é ilustrado, como exemplo, a constelação de um sinal QPSK no domínio do tempo contendo a fase e a amplitude correspondentes aos eixos I e Q. Esse sinal possui quatro pontos bem definidos nos valores 1 e -1. Quanto mais bem definidos esses pontos estiverem em relação aos seus valores originais, melhor será a qualidade do

sinal avaliado pelo cálculo da BER. O valor da BER deve ser menor que o valor definido no limite da FEC para recuperação das informações contidas no sinal.

Figura 5 - Constelação referente a um sinal sinalizado em QPSK previsto teoricamente.



Fonte: (SANTOS, 2020, p. 39)

2.1.3. Descrição do algoritmo de chave dinâmica

A descrição completa da DK é encontrada em (NGO, 2010). A explicação detalhada da geração da chave dinâmica para este trabalho foi realizada em (SOUZA, 2021). A explicação sobre a geração da DK em cifras de blocos é baseada na Figura 6. Considera-se que "Alice" é o transmissor e "Bob" é o receptor em um sistema de comunicação. A geração da chave dinâmica é baseada em três etapas:

1. Geração da chave inicial K_i e da chave temporária K_t, que são trocadas entre "Alice" e "Bob". A troca da chave pode ser realizada de diversas maneiras utilizando como exemplo as comunicações quânticas e, mais especificamente, a técnica QKD (LIAO, CAI e LIU, 2017). A troca pode ser realizada por meio das QKD por ser considerado uma via intrinsicamente segura pelas características do meio em que a chave será transmitida.
2. "Alice" e "Bob" geram a chave semente, K_s, a partir de uma função XOR entre as chaves K_t e K_i:

$$K_s = K_t \oplus K_i \tag{23}$$

3. A primeira chave dinâmica, DK_1, é gerado por "Alice" aplicando uma função de mão única, $f(x_1, x_2)$, à K_s e K_t:

$$DK_1 = f(K_s, K_t) \quad (24)$$

a. A segunda chave dinâmica, DK_2, é gerada aplicando a função de mão única à K_s e a DK_1:

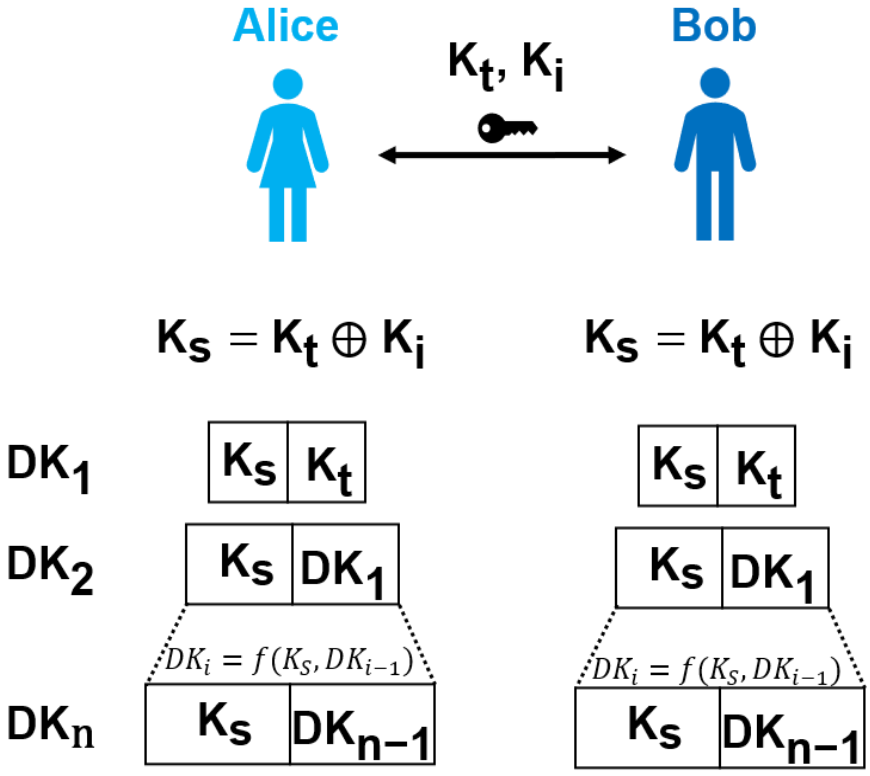
$$DK_2 = f(K_s, DK_1) \quad (25)$$

b. A terceira chave dinâmica é gerada aplicando a função de mão única à K_s e a DK_2. A operação continua até n-ésima chave dinâmica:

$$DK_n = f(K_s, DK_{(n-1)}) \quad (26)$$

c. O número de chaves dinâmicas geradas é definido pelo número de blocos que serão encriptados. Assim, se n é o número de chaves, podem ser encriptados no máximo n blocos.

Figura 6 - Esquemático ilustrativo e simplificado da geração de chaves dinâmicas.



Fonte: (SANTOS, 2020, p. 31).

A função de mão única tem aplicação no sentido direto de sua operação, porém no sentido inverso é relativamente difícil calcular. Neste trabalho, escolheu-se como função de mão única a função de *whirlpool* (SOUZA, NOGUEIRA, *et al.*, 2020). As chaves dinâmicas são possíveis de calcular apenas por "Alice" e por "Bob", que compartilham as chaves entre si. A chave de um bloco da chave dinâmica é sempre diferente da chave que foi utilizada no bloco anterior. Dessa forma, é possível satisfazer as propriedades de difusão e confusão de Shannon.

2.2. Rede óptica

No VPI, é possível simular cenários de transmissão e de detecção de sinais com diferentes características. Neste trabalho, foi desenvolvido um cenário de comunicação óptica com detecção coerente para simular a transmissão dos sinais em uma TON. Os sinais transmitidos, diferentemente do realizado já no trabalho em (ABBADE, NOGUEIRA, *et al.*, 2020), (NOGUEIRA, 2019) e (ABBADE; SOUZA *et al.*, 2020), podem assumir dupla polarização em X e Y com influência do efeito PMD. A composição da estrutura desenvolvida na rede óptica será descrita na Seção 2.2.1. O método realizado neste trabalho para otimização da potência do sinal na entrada dos MZM e da potência lançada na fibra óptica será explicado na Seção 2.2.2.

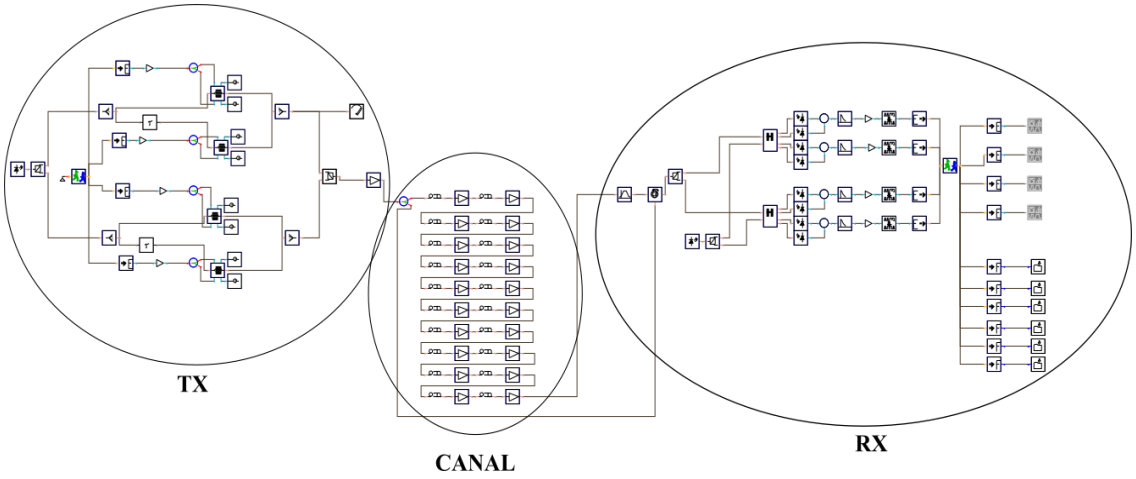
2.2.1. Estrutura da rede óptica

A estrutura completa para uma única rota da TON desenvolvida no VPI é mostrada na Figura 7. A explicação da estrutura será considerando apenas uma rota para uma comunicação ponto-a-ponto. Porém, os últimos resultados obtidos neste trabalho, Seção 3.2, são referentes a propagação por duas rotas, ou seja, foi adaptado essa estrutura para que fosse possível simular a transmissão de dois sinais de dupla polarização por duas rotas distintas. A estrutura é dividida em três partes, sendo o TX (Transmissor), CANAL e o RX (Receptor). Na Figura 8, Figura 9 e Figura 10, é mostrado cada uma dessas partes da estrutura para melhor visualização e entendimento, além de estar indicado os componentes utilizados na TON.

Na Figura 8, é mostrado o TX indicado na Figura 7. Os componentes que o TX contém são: laser de onda contínua (*Continuous Wave Laser*, laser CW); divisor de feixe de polarização (*polarisation beam splitter*, PBS); divisor e combinador de potência óptica; atenuador elétrico; MZM; fonte de alimentação de corrente contínua (*direct current*, DC) e um combinador de feixe de polarização (*polarisation beam combiner*, PBC).

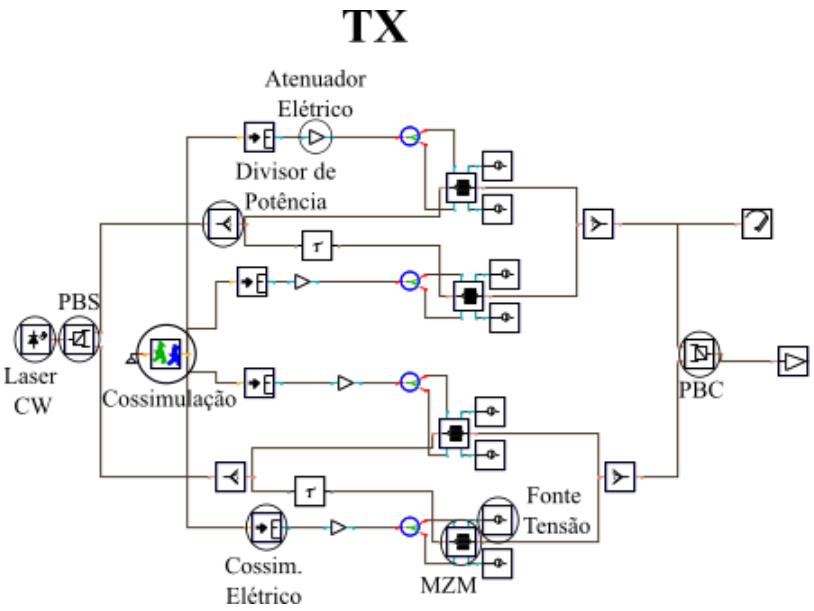
O círculo indicando a cossimulação na Figura 8 mostra o bloco responsável pela comunicação entre o Matlab e VPI. Na Figura 9, é mostrado o CANAL indicado na Figura 7. Os componentes que o CANAL contém são: fibra óptica padrão monomodo (*standard single mode fiber*, SSMF); EDFA e fibra compensadora de dispersão (*Dispersion Compensation Fiber*, DCF).

Figura 7 - Estrutura completa para simulação de uma rede de comunicação óptica com detecção coerente.



Fonte: Elaborado pelo autor.

Figura 8 - Estrutura do transmissor (TX) para simulação de uma rede de comunicação óptica com detecção coerente.

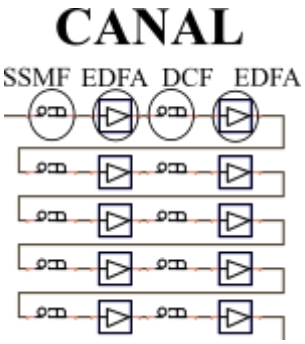


Fonte: Elaborado pelo autor.

Por último, na Figura 10, é apresentado o receptor (RX). Os componentes que o receptor possui são: filtro óptico passa-faixa; módulo de recuperação do estado de polarização ideal, que está indicado na figura como “controle de polarização”; PBS; oscilador local (*local oscilator*, LO); híbrida de 90°; fotodetectores (*photodetector*, PD); filtro elétrico; amplificador elétrico e bloqueador da componente DC do sinal. Após a recepção do sinal e realizada a demodulação do sinal será, então, enviado novamente para

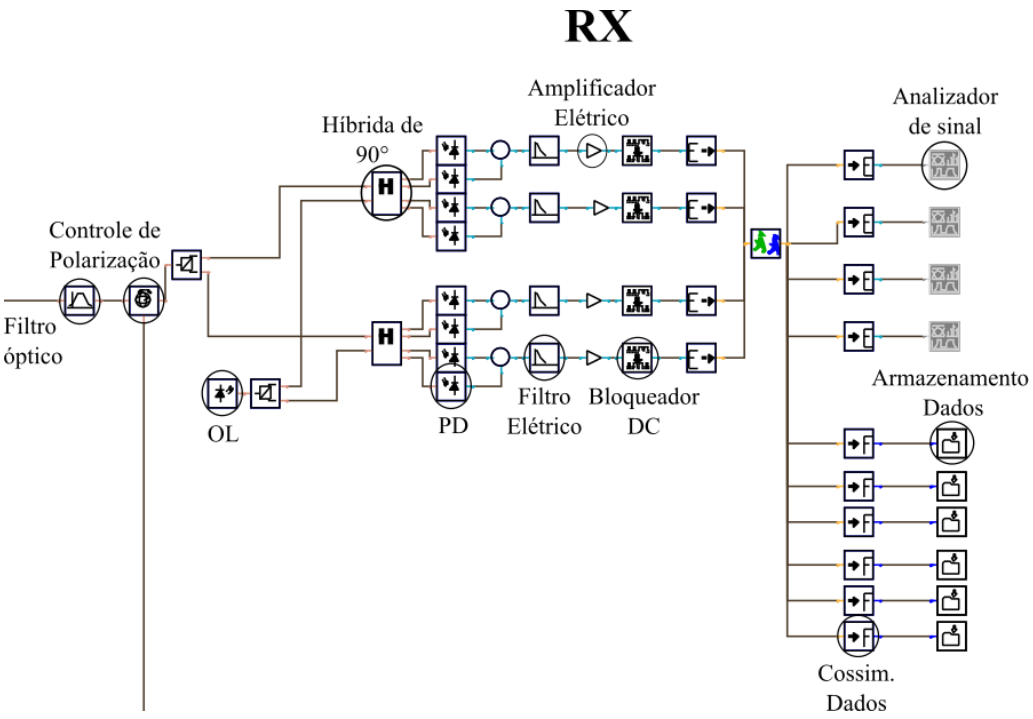
o ambiente Matlab pelo bloco da cossimulação para a descriptografia e recuperação do sinal.

Figura 9 - Estrutura do canal óptico para simulação de uma rede de comunicação óptica com detecção coerente.



Fonte: Elaborado pelo autor.

Figura 10 - Estrutura do receptor (RX) para simulação de uma rede de comunicação óptica com detecção coerente.



Fonte: Elaborado pelo autor.

As etapas que o sinal percorre durante a modulação, propagação e demodulação na comunicação óptica serão explicadas a seguir. O sinal criptografado é gerado no módulo “Transmissor” da Figura 1 e, utilizando a cossimulação entre o *software* Matlab e VPI, será enviado para o simulador da TON. O sinal criptografado possui duas polarizações ortogonais e é enviado em partes separadas, sendo a parte real e imaginária

de cada polarização X e Y. A parte real do sinal corresponde ao eixo I e a parte imaginária do sinal corresponde ao eixo Q. Os sinais criptografados real e imaginário na polarização X são nomeados de c_{X_I} e c_{X_Q}, respectivamente. Já na polarização Y, a parte real e imaginária são nomeadas como c_{X_I} e c_{Y_Q}, respectivamente.

Os sinais c_{X_I}, c_{X_Q}, c_{X_I} e c_{Y_Q} enviados para a TON são atenuados, e os valores de tensão das fontes de alimentação DC foram definidos de tal modo a ajustar o intervalo de tensão do sinal para passarem pelo MZM sem sofrerem penalidades significativos dos efeitos não lineares. No laser CW, é definido a frequência com que o sinal será modulado. Após os sinais passarem pelo modulador, foi utilizado um combinador de potência óptica para unir a parte real e imaginária dos sinais, que são denominados c_X e c_Y. Em seguida, os sinais nas polarizações X e Y são passados por um PBC. O sinal, após a combinação das polarizações, é chamado de c_{XY} e contém as informações nas polarizações X e Y.

A potência do sinal c_{XY} foi ajustada para ser lançada na SSMF. Na Figura 9, é mostrado um esquemático dos dispositivos utilizados para simular a transmissão. A SSMF aplica penalidades ao sinal, como atenuação, CD, PMD e efeitos não lineares. O EDFA realiza a compensação da atenuação, porém adiciona e amplifica o ruído do sinal. A DCF é utilizada para a compensação da CD, porém é necessário a adição de um segundo EDFA para compensar a atenuação causada pela DCF.

O sinal, após transmitido, passa por um filtro óptico passa-faixa, que limita a banda do ruído, um módulo de recuperação do estado de polarização ideal e um separador de polarização. O sinal é separado nas polarizações X e Y, resultando em c_X e c_Y. Os sinais c_X e c_Y são detectados de maneira coerente por uma híbrida de 90 graus. O laser do transmissor e do oscilador local do receptor possuem largura de linha nula, e assume-se que o oscilador e o laser de transmissão estão na mesma frequência (detecção homódina).

Os sinais são separados nos eixos I e Q e novamente nomeados como c_{X_I}, c_{X_Q}, c_{X_I} e c_{Y_Q}. Em seguida, são passados por um filtro elétrico passa-baixa para eliminar componentes espectrais de ruído externas à banda do sinal. Os sinais são, então, enviados para o módulo “Receptor”, pela cossimulação, onde é realizado o processo de descriptografia e ajuste das amplitudes para recuperação dos sinais.

2.2.2. Otimização da rede óptica

No decorrer do trabalho foi realizado um estudo diante da necessidade de ajustar dois parâmetros de grande importância na transmissão dos sinais pela rede óptica. O objetivo foi determinar os valores ótimos de atenuação ao sinal para estabelecer o melhor intervalo de tensão máximo do sinal na entrada do MZM e o melhor valor de potência de lançamento na fibra óptica. Nessa análise, foi utilizado um cenário mais simplificado considerando a geração de um sinal com dupla polarização e com aplicação da técnica de criptografia SPE-SS-DSP sem a utilização de chave dinâmica e sem a utilização da técnica de transmissão de sinais com taxas diferentes.

A criptografia SPE-SS-DSP foi aplicada a um sinal com duas polarizações ortogonais com os seguintes parâmetros: sinalização 16-QAM, taxa de símbolos (R_s) de 54 Gbaud para cada polarização, logo, uma taxa de transmissão de bits (R_b) igual a 432 Gbps para o sinal transmitido com as duas polarizações, número de símbolos de 16384 com duas amostras por símbolo, fator de decaimento de 0,02 e a banda codificada do sinal (B_c) de 27,54 GHz.

Os parâmetros da taxa de amostras e taxa de símbolos são definidos no *software* VPI sendo correspondentes e em acordo com os utilizados no *software* KryptusSJ. O comprimento de enlace de fibra óptica utilizada foi de 770 km, sendo 11 conjuntos de 70 km de SSMF, um EDFA e 12,44 km de DFC em cascata. Os valores dos parâmetros referentes a dispersão, atenuação e do coeficiente dos efeitos não lineares foram de 16 ps/(nm·km), 0,2 dB/km e $2{,}6 \cdot 10^{-20}$ (m^2/W), respectivamente para a SSMF.

A figura de ruído do EDFA foi ajustada para 4,4 dB. O efeito da PMD da SSMF e da DCF foi excluído da simulação, sendo o coeficiente da PMD definido como nulo para entender melhor o funcionamento da TON desenvolvida e possibilitar, após a otimização dos parâmetros em questão, a minimização das penalidades ocasionadas ao sinal transmitido. O parâmetro de dispersão, atenuação e do efeito não linear utilizada na DCF foi de -100 ps/(nm·km), 0,2 dB/km e $2{,}6 \cdot 10^{-20}$ (m^2/W).

A banda do filtro passa faixa óptico foi definida sendo 4 vezes a taxa de símbolos. Nos fotodetectores foram definidos o parâmetro de ruído térmico branco com valor de 10 pA/$Hz^{1/2}$. A largura de banda dos filtros elétricos passa baixa foi definida como 70 % da taxa de símbolos. O processo de otimização foi realizado fixando o comprimento em 700 km para análise do comportamento da BER próximo ao limite da FEC de $2 \cdot 10^{-3}$.

O processo de otimização foi dividido em quatro etapas. Na primeira etapa (i), um valor inicial de 6,20 dB foi definido para o atenuador elétrico na entrada do MZM, com base no trabalho desenvolvido em (NOGUEIRA, BADUE, *et al.*, 2023). Na segunda etapa (ii), a potência de lançamento na fibra foi varrida até atingir valores que resultaram em valores de BER próximos ao limite da FEC. Os intervalos limites de potência de lançamento da fibra encontrados foram de -6 a -2 dBm para o sinal sem criptografia e de -5 a -1 dBm para o sinal criptografado. A terceira etapa (iii) envolveu a varredura dos valores de atenuação elétrica aplicada aos sinais criptografados e não criptografados na entrada do MZM para cada potência de lançamento na fibra encontrada na segunda etapa.

Os valores de atenuação aplicados para os sinais sem criptografia variaram o intervalo de tensão do sinal de 0,6 a 3,96 volts (V). Enquanto para os sinais criptografados, os valores de atenuações variaram o intervalo máximo de tensão de 1,32 a 7,29 V. Nos sinais criptografados, foi obtido um intervalo máximo de tensão maior e, portanto, foram mais suscetíveis aos efeitos não lineares do MZM, resultando em limites de intervalo máximo de tensão menores em comparação com os sinais sem criptografia.

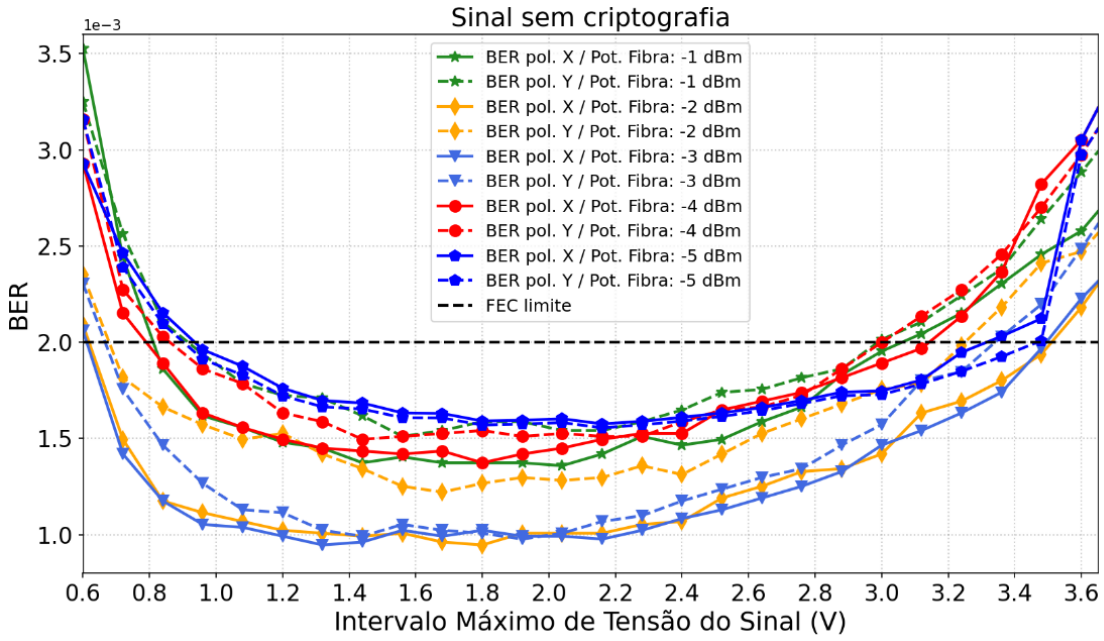
Na Figura 11 e a Figura 12, é apresentado os resultados relativos à BER dado um valor de intervalo máximo de tensão na entrada do MZM para os sinais não criptografados e para os sinais criptografados e descriptografados, respectivamente. As cores e os símbolos das curvas correspondem a potência de lançamento na fibra, variando de -1 a -5 dBm para os sinais sem criptografia e, de -2 a -6 dBm para os sinais com criptografia.

As curvas tracejadas correspondem a polarização X e as curvas contínuas correspondem a polarização Y. No ponto ótimo para os sinais sem criptografia, foi obtido uma potência de lançamento na fibra de -3 dBm para um intervalo de tensão máximo de 1,32 V e uma BER próxima de $1 \cdot 10^{-3}$. Nos sinais criptografados e descriptografados, o ponto ótimo teve uma potência de lançamento na fibra de -4 dBm para um intervalo máximo de tensão de 3,64 V e uma BER próxima a $0{,}7 \cdot 10^{-3}$.

Na quarta etapa (iv), foi verificado se os limites definidos para a potência de lançamento na fibra óptica, baseados no valor inicial de atenuação escolhido, foram coerentes. A partir dos valores ótimos do intervalo máximo de tensão, foi realizado uma varredura da potência de lançamento na fibra para os sinais sem criptografia de -6 a 0 dBm e, para os sinais criptografados e descriptografados de -7 a -1 dBm. Os resultados

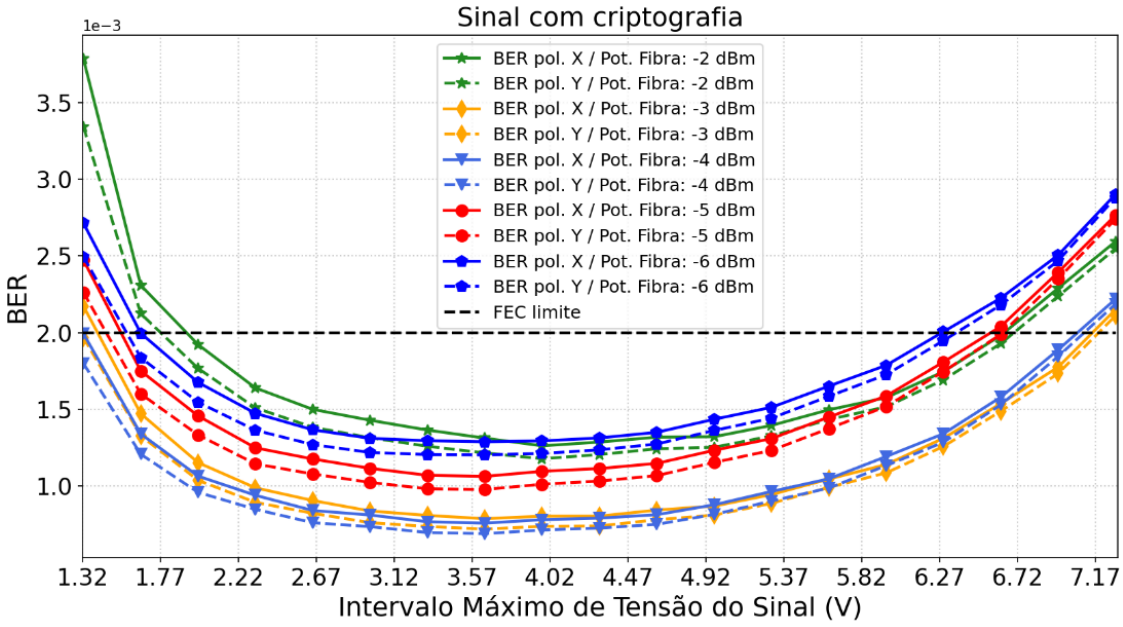
obtidos para os sinais criptografados são mostrados nas Figura 13 e, os resultados para os sinais criptografados e descriptografados são mostrados na Figura 14.

Figura 11 - Otimização do intervalo máximo de tensão do sinal sem criptografia na entrada do Modulador Mach-Zehnder.



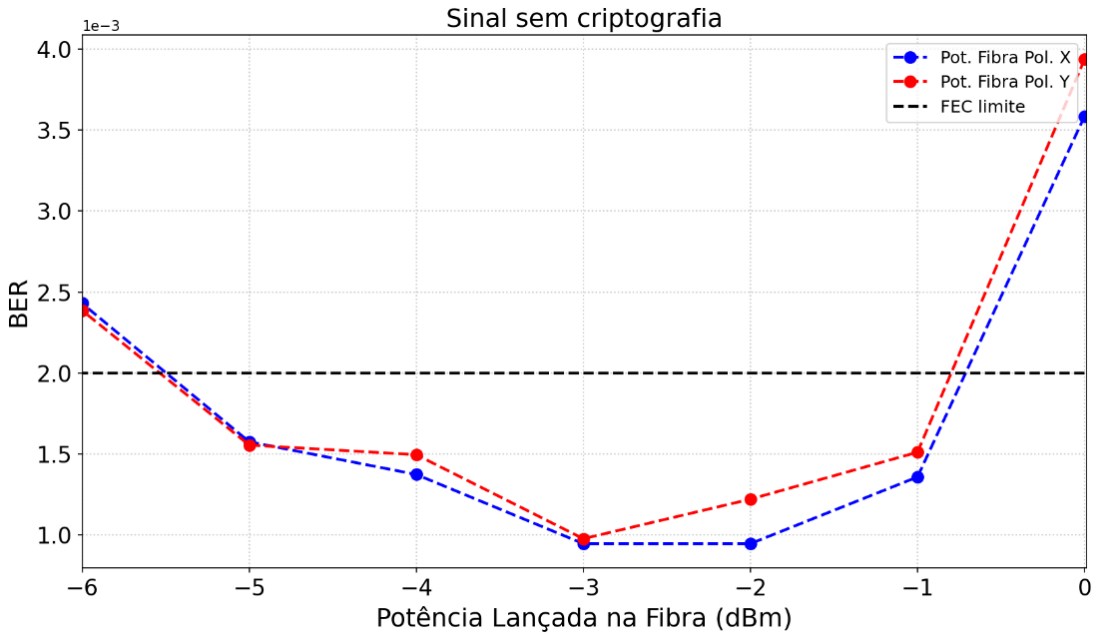
Fonte: Elaborado pelo autor.

Figura 12 - Otimização do intervalo máximo de tensão do sinal com criptografia na entrada do Modulador Mach-Zehnder.



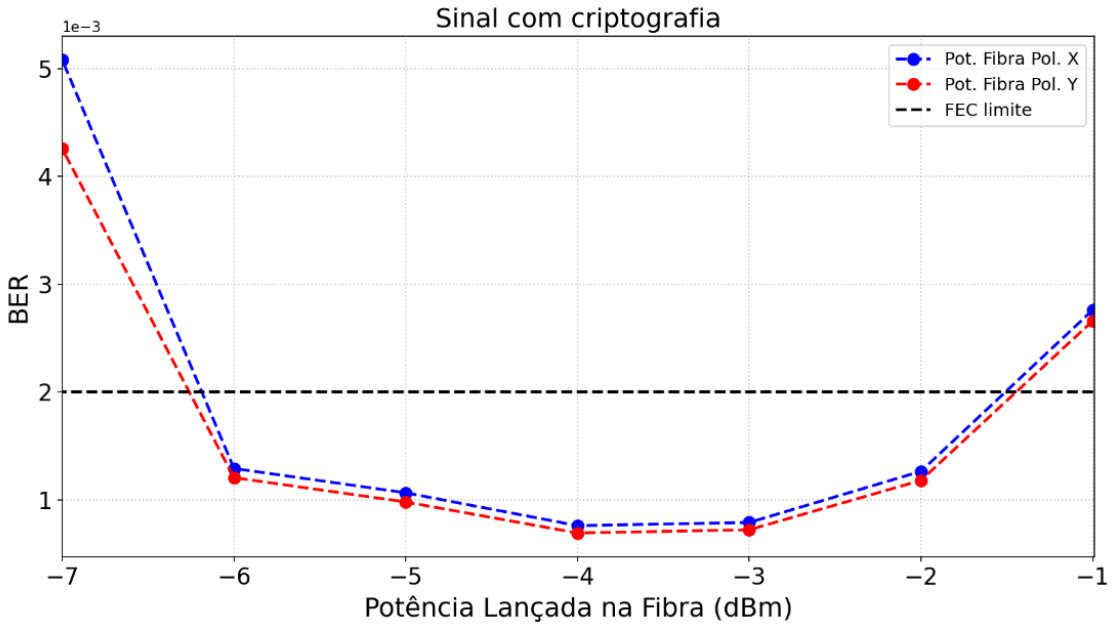
Fonte: Elaborado pelo autor.

Figura 13 - Otimização da potência de lançamento na fibra óptica para sinal sem criptografia.



Fonte: Elaborado pelo autor.

Figura 14 - Otimização da potência de lançamento na fibra óptica para sinal com criptografia.



Fonte: Elaborado pelo autor.

Nas Figura 13 e Figura 14, os valores ótimos obtidos das potências de lançamento na fibra óptica foram -3 dBm e -4 dBm para o sinal não criptografado e sinal criptografado

e descriptografado, respectivamente. A Tabela 2 contém um resumo dos resultados obtidos, contendo os valores dos pontos ótimos encontrados.

Tabela 2 - Valores ótimos de atenuação aplicado ao sinal, intervalo máximo de tensão do sinal e potência de lançamento na fibra óptica.

Sinal	Atenuação [dB]	Intervalo máximo de tensão do sinal [V]	Potência lançada na fibra óptica [dBm]
Sem criptografia	6,58	1,32	-3
Com criptografia	6,58	3,64	-4

Fonte: Elaborado pelo autor.

3. RESULTADOS

Os resultados das adaptações e melhorias incorporadas ao código desenvolvido por Nogueira (NOGUEIRA, 2022) são descritos e mostrados neste capítulo, que está dividido em duas seções. Na primeira Seção 3.1, são apresentados os resultados da transmissão em uma única rota de um sinal de dupla polarização, gerado com taxas de transmissão de símbolo distintas, criptografado com SPE-SS-DSP e utilizando DK. O objetivo desses resultados foi validar o cenário de comunicação óptico desenvolvido e descrito na Seção 2.2.

Na Seção 3.2, são apresentados os resultados da transmissão de dois sinais de dupla polarização, criptografados com SPE-SS-Scr-DSP e utilizando DK. Ambos os sinais foram gerados com diferentes taxas de transmissão de símbolo e sinalizações para validação final de todas as melhorias e adaptações realizadas no decorrer deste trabalho. Em ambas as seções, os resultados mostrados são importantes para compreender o comportamento dos sinais transmitidos, permitindo a comparação entre os sinais criptografados, descriptografados e não criptografados. Destaca-se, na Seção 3.2, que os sinais criptografados foram transmitidos com modulações distintas, o que introduz um comportamento novo para análise.

Os parâmetros definidos e otimizados para a estrutura da TON, descritos na Seção 2.2.2, exceto o efeito PMD, foram aplicados nos cenários de simulações realizados nas Seções 3.1 e 3.2. Nos resultados obtidos, foram mantidos 70 km de segmento de fibra óptica para cada iteração simulada até atingir valores da BER próximos do limite da FEC. O coeficiente do efeito PMD foi adicionado nas simulações e definido em $3{,}16 \cdot 10^{-15}$ s/√m. A principal métrica adotada para estimar a qualidade do sinal foi o cálculo da BER em relação ao comprimento de enlace da fibra óptica.

O número de blocos, n_b, foi definido como 32; o fator de decaimento do RCF, r, foi configurado como 0,002, e o número de amostras por símbolo foi definido igual a 2. Esses parâmetros foram mantidos no código para os resultados obtidos nas Seções 3.1 e 3.2. Os demais parâmetros do código foram específicos para cada sinal gerado e serão descritos nas Seções 3.1 e 3.2 separadamente.

Os espectros e constelações obtidos correspondem aos 140 km percorridos de fibra óptica. Em ambas as seções, são apresentados resultados dos espectros e constelações dos sinais gerados, criptografados e descriptografados, representados pelas letras “m”, “c” e

“d”, respectivamente. Os sinais modulados e transmitidos pela fibra óptica serão representados pela letra “t” e, para esses sinais, foram obtidos apenas os espectros em frequência.

3.1. Propagação de sinal com dupla polarização por uma única rota

Os primeiros resultados obtidos correspondem à transmissão por apenas uma única rota de um sinal de dupla polarização, criptografado em SPE-SS-DSP e utilizando DK. Os parâmetros específicos de cada sinal, definidos no código, são mostrados na Tabela 3 a seguir. Esses parâmetros incluem a sinalização utilizada, taxa de transmissão de símbolo, taxa de transmissão de bit, banda codificada, número de símbolos e número de amostras.

Tabela 3 – Parâmetros definidos para a geração de um bloco correspondente aos sinais propagados por um única rota.

Sinal	Sinalização	R_s $(GBaud)$	R_b (Gb/s)	B_c (GHz)	Número de símbolos	Número de amostras
$S_{1,X}$	16QAM	28	112	14,28	512	1024
$S_{1,Y}$	16QAM	42	168	21,42	1024	2048

Fonte: Elaborado pelo autor.

Os sinais gerados, após a aplicação da técnica para taxas de transmissão distintas, têm a taxa de símbolos do sinal na polarização em X igual à da polarização em Y. Assim, ambas as polarizações possuem taxas de transmissão iguais a 42 Gbaud e número de símbolos igual a 32768. Essa técnica é aplicada justamente para permitir a transmissão de sinais gerados com taxas diferentes (NOGUEIRA, 2022).

Após a recuperação e descriptografia do sinal no receptor, os sinais retornam às suas características iniciais, ou seja, o sinal na polarização em X retorna à taxa de símbolo de 28 Gbaud com 16384 símbolos, enquanto o sinal na polarização em Y retorna à taxa de símbolo de 42 Gbaud com 32768 símbolos. Na Figura 15, são observadas essas mudanças entre o sinal gerado, sinal criptografado e o sinal descriptografado e recuperado. Os espectros e as constelações do sinal nas polarizações X e Y foram obtidos em quatro etapas:

1) Na primeira etapa, foram obtidos os sinais gerados pela função “Mapeador” (Figura 15(a) e Figura 15(b)). Os símbolos que identificam os sinais nessa etapa

são $m_{1,X}$ e $M_{1,X}$ para o sinal na polarização X, e $m_{1,Y}$ e $M_{1,Y}$ para o sinal na polarização Y.

2) Na segunda etapa, foram obtidos os sinais após aplicado as técnicas de criptografia (Figura 15(c) e Figura 15(d)). Os símbolos que identificam os sinais nessa etapa são $c_{1,X}$ e $C_{1,X}$ para a polarização X, e $c_{1,Y}$ e $C_{1,Y}$ para a polarização Y.
3) Na terceira etapa, foi obtido apenas o espectro do sinal transmitido pela fibra óptica (Figura 16 (e)). O símbolo que identifica o sinal nessa etapa é $T_{1,XY}$.
4) Na quarta etapa, foram obtidos os sinais recuperados e descriptografados após a função "Demapeador" (Figura 15(e) e Figura 15(f)). Os símbolos que identificam os sinais nessa etapa são $d_{1,X}$ e $D_{1,X}$ para a polarização X, e $d_{1,Y}$ e $D_{1,Y}$ para a polarização Y.

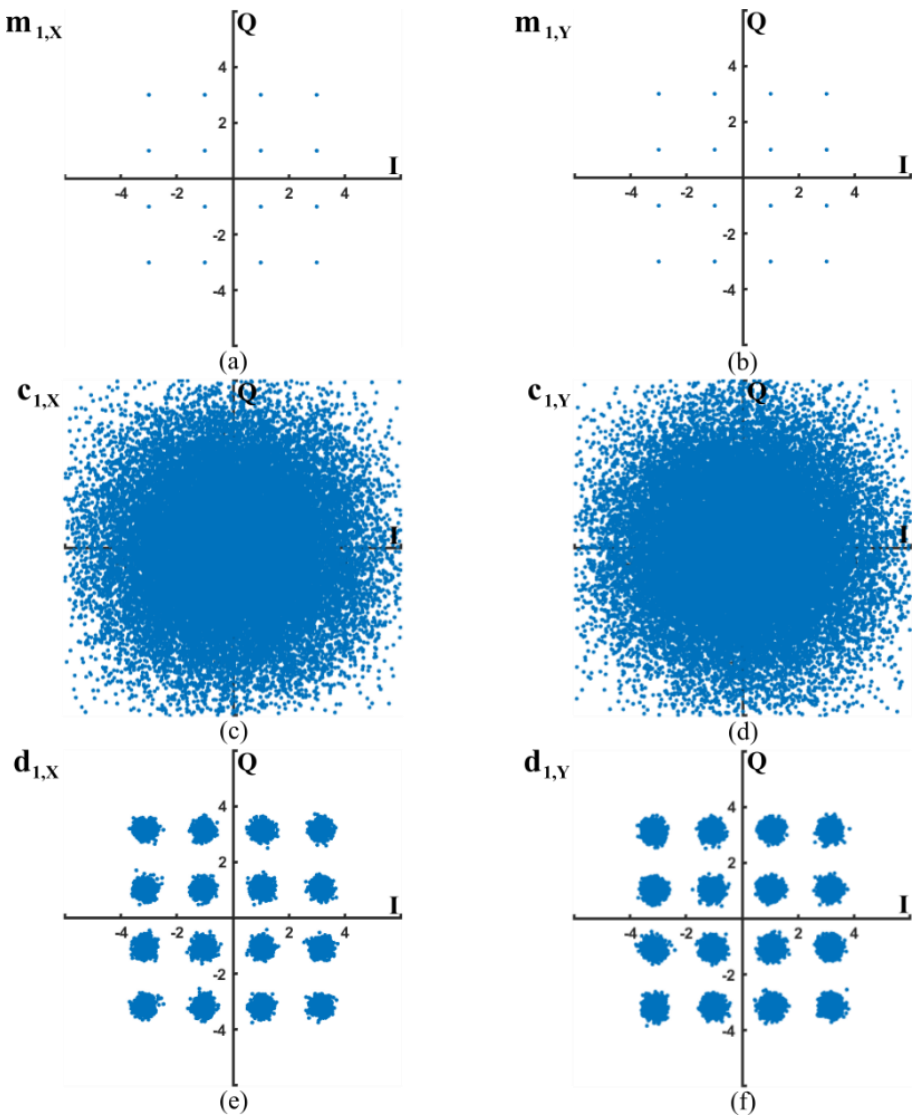
Os resultados obtidos referentes às constelações e aos espectros são mostrados na Figura 15 e Figura 16, respectivamente. Os pontos das Figura 15(a) e Figura 15(b) estão bem definidos nas amplitudes de 1, -1, 3, -3 para os sinais gerados e sinalizados em 16QAM. As constelações das Figura 15(c) e Figura 15(d) correspondem aos sinais criptografados e possuem uma distribuição de amplitude aproximadamente gaussiana nos eixos I e Q. Na Figura 15(e) e Figura 15(f), são mostrados os sinais, após a transmissão por 140 km, recuperados e descriptografados.

Nessas duas últimas figuras, observa-se que houve adição de ruído ao sinal durante a transmissão, resultando em uma qualidade que não é mais a mesma do sinal gerado inicialmente, ou seja, os pontos das constelações mostrados na Figura 15(e) e Figura 15(f) já não estão tão bem definidos como os pontos das constelações mostrados na Figura 15(a) e Figura 15(b). Porém, os sinais recuperados e descriptografados, mesmo com os pontos não tão bem definidos como os sinais originais, possuem valores baixos de BER, em torno de 10^{-11}, sendo possível a recuperação dos sinais.

Na Figura 16(a) e Figura 16(b), são mostrados os espectros em frequência dos sinais complexos gerados em banda base na função "Mapeador". Os sinais, nessa etapa, ainda não foram criptografados, não passaram pelo RCF e as taxas de transmissão de símbolo não foram ajustadas. Ambos os sinais, nas polarizações em X e Y, possuem larguras de banda diferentes. Na Figura 16(c) e Figura 16(d), são mostrados os espectros em frequência dos sinais passados pelo RCF, criptografados e com as taxas de transmissão de símbolos e larguras de banda igualadas.

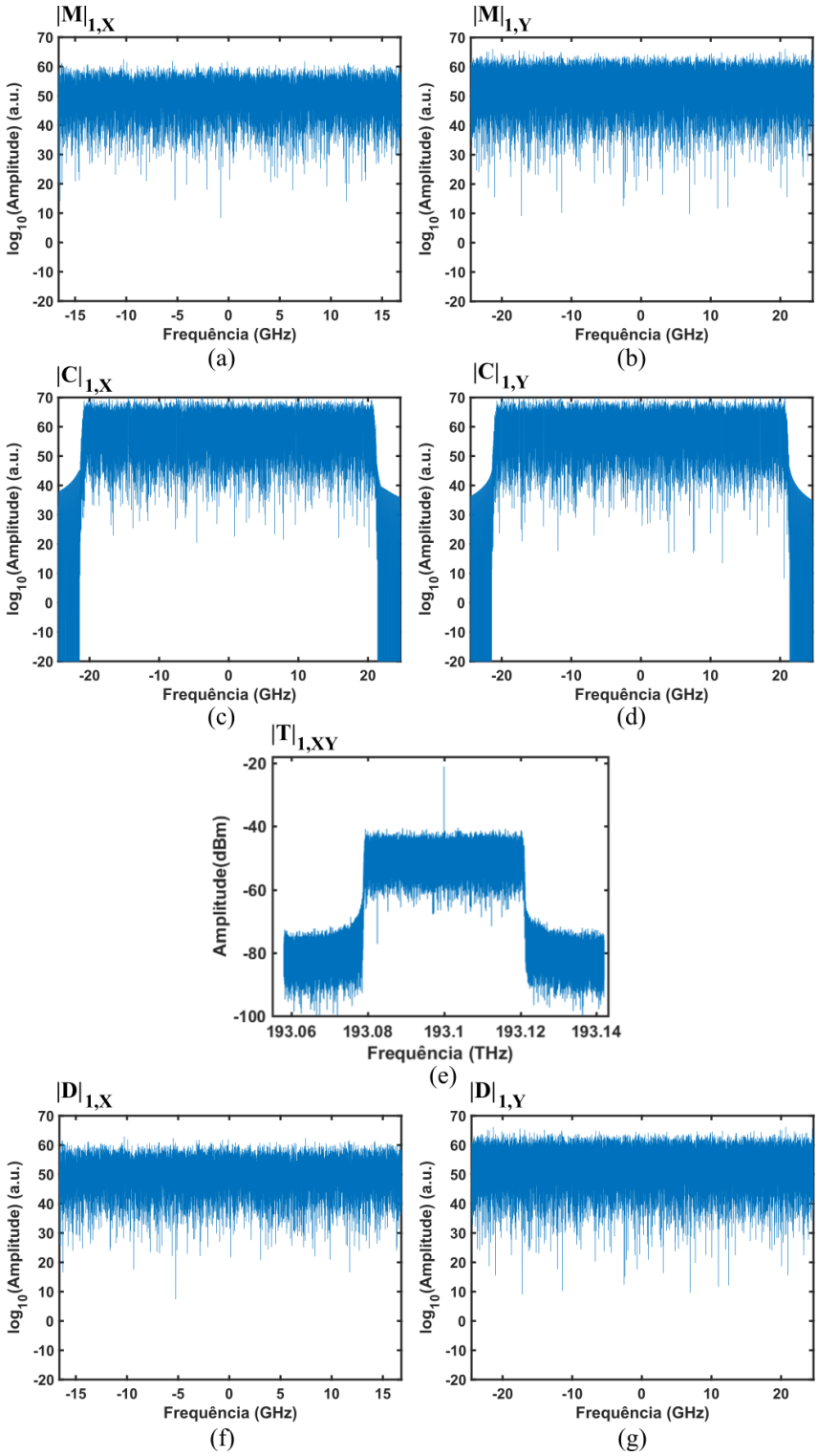
Em ambas as figuras, Figura 16(c) e Figura 16(d), percebe-se que as características dos sinais são muito similares e não é possível distinguir qual o sinal foi gerado com taxa de símbolo e largura de banda menor, tornando a transmissão dos sinais mais segura. Na Figura 16(e), é mostrado o espectro do sinal modulado e transmitido pela fibra óptica, contendo as polarizações X e Y. Na Figura 16(f) e Figura 16(g), são mostrados os espectros referentes aos sinais descriptografados e recuperados, com largura de banda, taxa de transmissão de símbolo e o número de símbolos retornados aos valores originais.

Figura 15 - Constelações obtidas e correspondentes ao sinal gerado inicialmente na entrada na (a) polarização X e na (b) polarização Y, sinal criptografado na (c) polarização X e na (d) polarização Y, sinal descriptografado e recuperado na (e) polarização X e na (f) polarização Y.



Fonte: Elaborado pelo autor

Figura 16 - Espectros de amplitude obtidos e correspondentes ao sinal gerado inicialmente na (a) polarização X e na (b) polarização Y, sinal criptografado na (c) polarização X e na (d) polarização Y, (e) sinal criptografado e transmitido contendo as polarizações X e Y, sinal descriptografado e recuperado na (f) polarização X e na (g) polarização Y.



Fonte: Elaborado pelo autor.

Na Figura 17, é apresentado o resultado obtido da propagação de um sinal de dupla polarização pela TON por meio de uma única rota. As constelações do sinal descriptografado e recuperado, correspondente à polarização X, estão indicadas na figura, como exemplo, nos pontos de 140 e 700 km de fibra óptica. A constelação indicada a 350 km refere-se ao sinal criptografado na polarização X que foi transmitido pela fibra óptica.

As nomenclaturas adotadas para as siglas utilizadas na Figura 17 e Figura 22 diferem das utilizadas para as constelações e espectros, pois são destacadas curvas referentes aos sinais transmitidos com a aplicação das técnicas de criptografias e curvas referentes aos sinais transmitidos sem a aplicação dessas técnicas, permitindo uma comparação e avaliação entre elas. Os significados das siglas utilizadas nessas figuras são descritos a seguir:

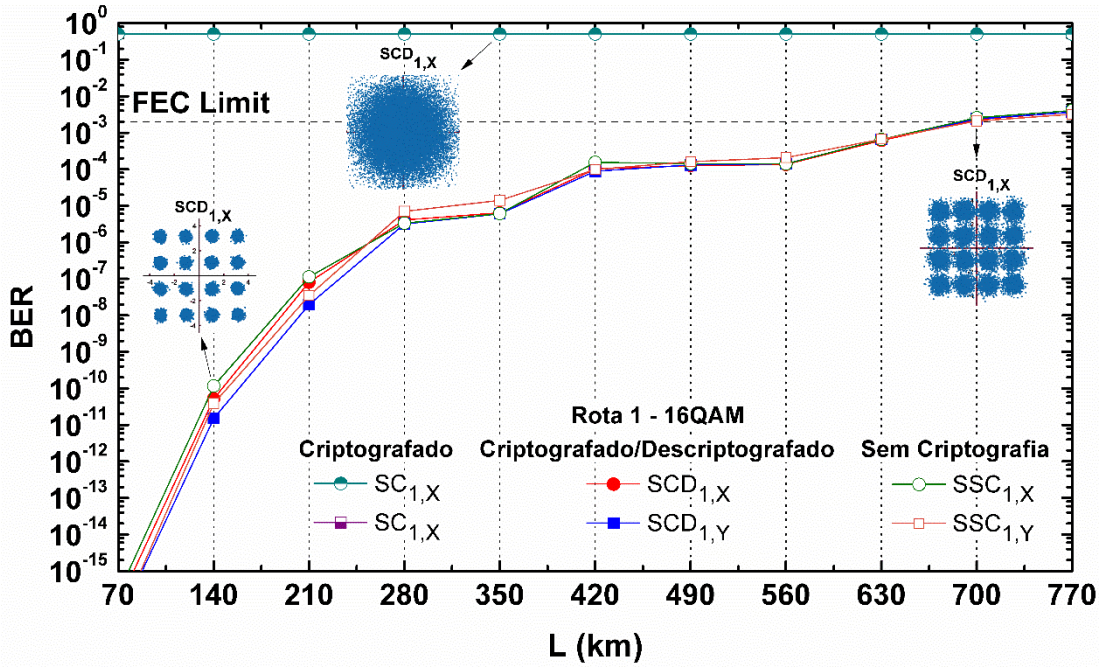
1) SSC: Sinal Sem Criptografia;
2) SC: Sinal Criptografado;
3) SCD: Sinal Criptografado e Descriptografado.

O subscrito nessas siglas mantém as definições adotadas no Capítulo 2. A letra representando o sinal pode ser acompanhada pelo número associado ao sinal gerado, que identifica a rota pela qual o sinal será propagado; pela polarização correspondente, que pode ser X ou Y; pelo tipo de sinalização utilizado (QPSK ou 16QAM); e pela parte real (eixo I) ou pela parte imaginária (eixo Q) do sinal. Portanto, a sigla, como, por exemplo, $SCD_{1,X,}$ indica o primeiro sinal criptografado e descriptografado na polarização X, transmitido pela primeira rota (Rota 1), enquanto $SCD_{2,Y}$ indica o segundo sinal criptografado e descriptografado na polarização Y, transmitido pela segunda rota (Rota 2).

Na Figura 17, as curvas correspondentes aos sinais SSC e SCD mostraram um comportamento muito similar e com valores de BER muito próximos. O comprimento da fibra óptica alcançado por esses sinais, no qual a BER corresponde ao limite da FEC, foi praticamente o mesmo, sendo de 700 km e muito próxima do estudo realizado em (ABBADE, NOGUEIRA, *et al.*, 2020). As técnicas de criptografia e as adaptações realizadas no código, em conjunto com a adição do efeito PMD, não causaram uma penalidade significativa para os SCD quando comparados aos SSC. No entanto, é importante destacar que as adaptações e melhorias realizadas neste trabalho para obter o melhor resultado aumentaram o tempo de simulação. O aumento da complexidade ao

introduzir o algoritmo responsável pela recuperação das amplitudes do sinal, descrito na Seção 2.1.2, em conjunto com as técnicas de criptografia, DK, transmissão de sinais gerados com taxas diferentes e cálculo da BER resultam em maior tempo de processamento quando comparada aos cenários *back-to-back*.

Figura 17 - Gráfico dos valores da BER dado um comprimento de fibra óptica para um sinal com dupla polarização criptografado em SPE-SS-DSP e não criptografado sendo propagado por uma TON.



Fonte: Elaborado pelo autor.

O tempo, por exemplo, demandado para a simulação completa e obtenção dos dados referentes à Figura 17 foi em torno de 6 horas, e o tempo de simulação demandado para cada segmento da fibra óptica até atingir o limite da FEC é aproximadamente 15 minutos. No cenário *back-to-back*, as simulações demoraram poucos segundos para serem executadas, em torno de 60 a 120 segundos. No tempo demandando nesses dois cenários, não foi considerado o tempo para geração das chaves criptográficas que é em torno de 5,5 minutos. Porém, as chaves são salvas em um arquivo, possibilitando o carregamento delas no decorrer do código de forma rápida. Logo, esse tempo demandado para a geração das chaves seria apenas para a primeira simulação. Os parâmetros definidos também influenciam o tempo de simulação, como número de símbolos, números de amostras e o número de blocos que o sinal contém. Caso esses parâmetros possuam valores baixos, a simulação é mais rápida.

3.2. Propagação de dois sinais com dupla polarização por duas rotas

Os resultados obtidos nesta seção correspondem à transmissão por duas rotas diferentes de um sinal de dupla polarização, criptografado em SPE-SS-Src-DSP e utilizando DK. Os parâmetros definidos no código para a geração do primeiro sinal, criptografado ou não criptografado, com dupla polarização para a primeira e segunda rota são mostrados na Tabela 4. Esses parâmetros são os mesmos descritos na seção anterior, na Tabela 3.

Tabela 4 – Parâmetros definidos para a geração de um bloco correspondente aos sinais propagados por duas rotas.

Sinal	Sinalização	R_s $(GBaud)$	R_b (Gb/s)	B_c (GHz)	Número de símbolos	Número de amostras
$S_{1,X}$	QPSK	28	56	14,28	512	1024
$S_{1,Y}$	QPSK	28	56	14,28	512	1024
$S_{2,X}$	16QAM	42	168	21,42	1024	2048
$S_{2,Y}$	16QAM	42	168	21,42	1024	2048

Fonte: Elaborado pelo autor.

Os sinais gerados para transmissão pela primeira rota, após concatenados os 32 blocos, possuem 16384 símbolos, correspondendo a 32768 amostras. Enquanto os sinais gerados para transmissão pela segunda rota, após concatenados os 32 blocos, possuem 32768 símbolos, correspondendo a 65536 amostras. Os sinais gerados, após a aplicação da técnica para taxas de transmissão distintas, têm a taxa de símbolos do primeiro sinal na polarização X e Y igual à do segundo sinal na polarização X e Y, ou seja, todos os sinais foram transmitidos com a mesma R_s, B_c, número de símbolos e número de amostras, sendo iguais a 42 Gbaud, 21,42 GHz, 32768 e 65536, respectivamente. Após a descriptografia e recuperação do sinal no receptor, os sinais retornaram às suas características originais.

Os sinais modulados em QPSK foram propagados pela primeira rota, variando o comprimento de enlace da fibra óptica até atingir o valor da BER correspondente ao limite da FEC. Os sinais modulados em 16QAM foram propagados pela segunda rota, com o comprimento de enlace da fibra óptica fixado em 420 km. A transmissão dos sinais por rotas distintas, em caso de intrusão, dificulta a descriptografia, pois, como as componentes estão embaralhadas entre os sinais, seria necessário obter todos os sinais

propagados pelas duas rotas para a realização da descriptografia e recuperação das informações presentes nos sinais transmitidos (ABBADE, NOGUEIRA, *et al.*, 2020).

Nas Figura 18, Figura 19, Figura 20 e Figura 21, são mostradas as constelações e espectros dos sinais gerados, criptografados e dos sinais descriptografados e recuperados. As constelações dos sinais relativas à primeira e segunda rota são mostradas nas Figura 18 e Figura 19, respectivamente. Já os espectros dos sinais para a primeira e segunda rota são apresentados nas Figura 20 e Figura 21, respectivamente

Os espectros e as constelações do sinal na polarização X e Y foram obtidos em quatro etapas, conforme descrito na seção anterior. No entanto, nesta seção, foram considerados os resultados obtidos para dois sinais com dupla polarização transmitidos por duas rotas. Logo, além de considerar resultados obtidos para os sinas referentes à primeira rota, $m_{1,Y}$, $M_{1,Y}$, $c_{1,X}$, $C_{1,X}$, $c_{1,Y}$, $C_{1,Y}$, $T_{1,XY}$, $d_{1,X}$, $D_{1,X}$, $d_{1,Y}$, $D_{1,Y}$, também foram obtidos os sinais referentes à segunda rota, que são $m_{2,Y}$, $M_{2,Y}$, $c_{2,X}$, $C_{2,X}$, $c_{2,Y}$, $C_{2,Y}$, $T_{2,XY}$, $d_{2,X}$, $D_{2,X}$, $d_{2,Y}$, $D_{2,Y}$.

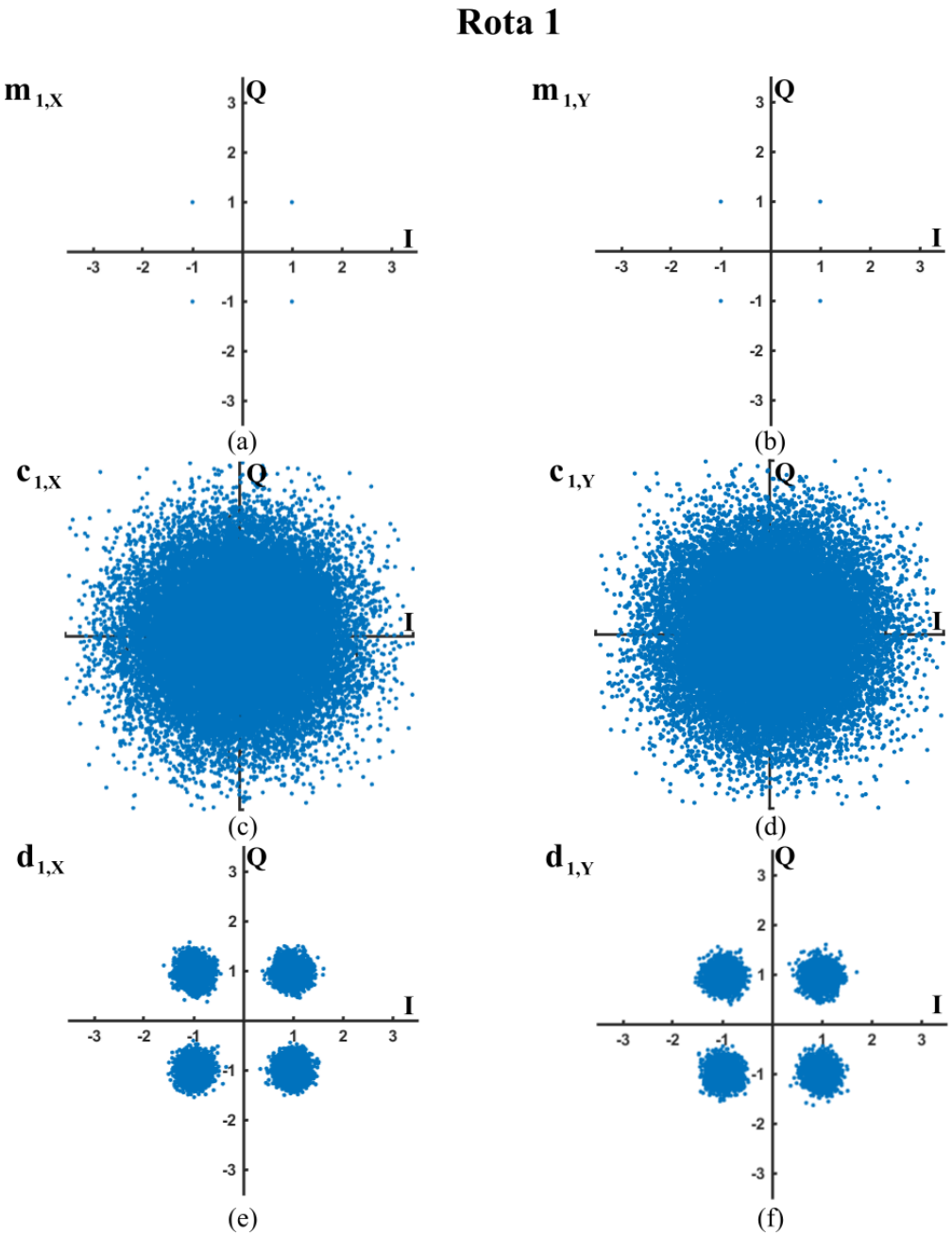
Os pontos das constelações na Figura 18(a) e Figura 18(b) estão bem definidos nas amplitudes de -1 e 1 para os sinais gerados e sinalizados em QPSK. As constelações na Figura 18(c) e Figura 18(d) correspondem aos sinais criptografados e possuem uma distribuição de amplitude aproximadamente gaussiana nos eixos I e Q. Na Figura 18(e) e Figura 18(f), são mostrados os sinais recuperados e descriptografados após a transmissão por 140 km de fibra óptica.

A adição de ruído nos sinais durante a propagação pela TON é notada na Figura 18(e) e Figura 18(f) pela distribuição gaussiana dos pontos ao redor dos valores 1 e -1. As amplitudes dos sinais descriptografados e recuperados já não estão tão bem definidas como as amplitudes das constelações mostradas na Figura 18(a) e Figura 18(b). Porém, os sinais recuperados e descriptografados, possuem valores baixos de BER, em torno de 10^{-10}, sendo possível a recuperação dos sinais. As constelações referentes aos sinais propagados pela segunda rota são mostradas na Figura 19.

Os pontos das constelações das Figura 19(a) e Figura 19(b) estão bem definidos nas amplitudes de -3, -1, 1 e 3 para os sinais gerados e sinalizados em 16QAM. Assim como descrito na Figura 18, as constelações mostradas na Figura 19(c) e Figura 19(d) correspondem aos sinais criptografados e possuem uma distribuição de amplitude aproximadamente gaussiana nos eixos I e Q. As constelações da Figura 19(e) e Figura

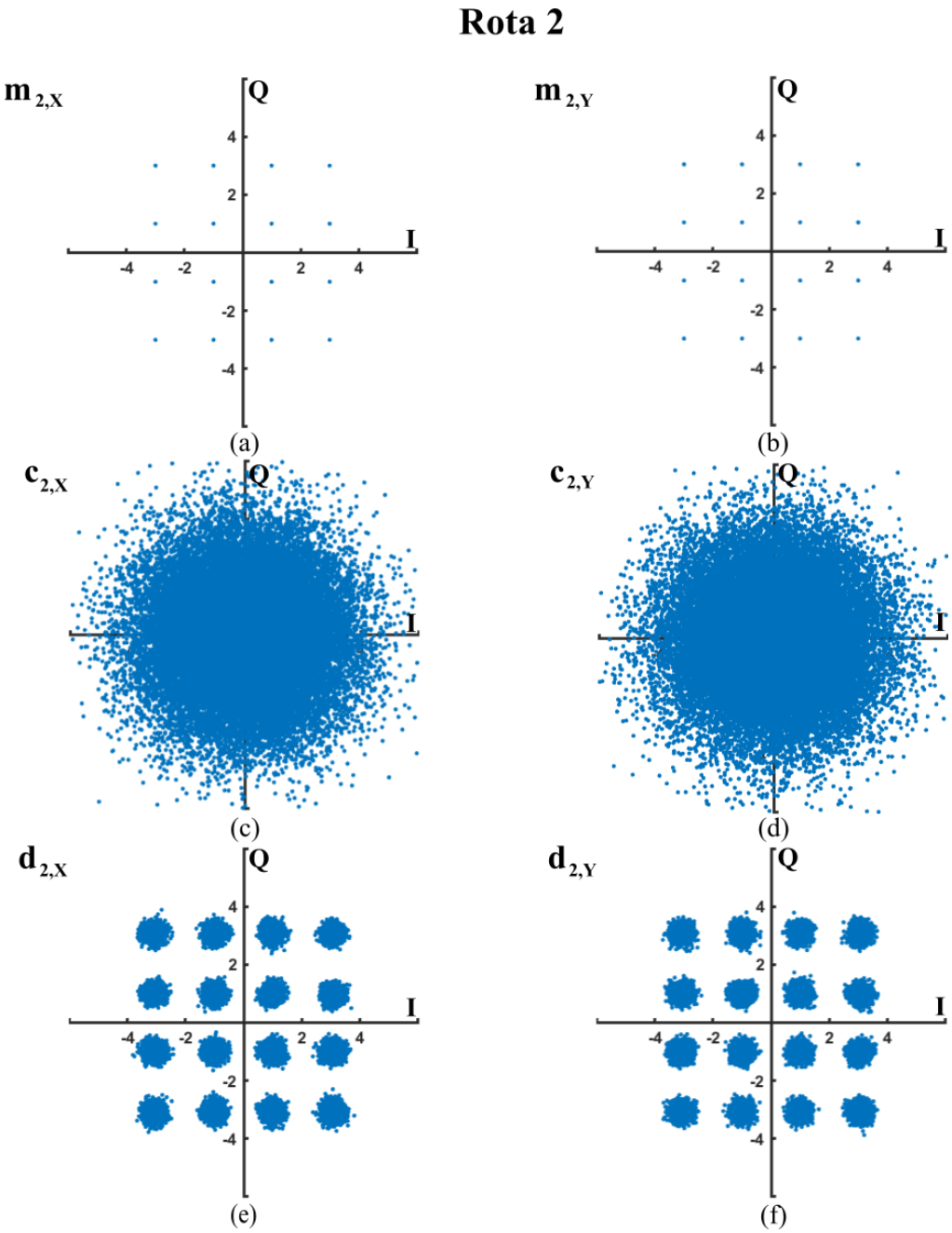
19(f) correspondem aos sinais descriptografados e recuperados após a propagação por 140 km de fibra óptica. Os sinais descriptografados e recuperados, mesmo com a presença do ruído, possuem valores baixos de BER, em torno de 10^{-10}, o que torna possível a recuperação das informações contidas nos sinais.

Figura 18 - Constelações obtidas referente a primeira rota de propagação correspondendo ao sinal gerado inicialmente na (a) polarização X e na (b) polarização em Y, sinal criptografado na (c) polarização X e na (d) polarização Y, sinal descriptografado e recuperado na (e) polarização X e na (f) polarização Y.



Fonte: Elaborado pelo autor.

Figura 19 - Constelações obtidas referentes a segunda rota de propagação correspondendo ao sinal gerado inicialmente na (a) polarização X e na (b) polarização em Y, sinal criptografado na (c) polarização X e na (d) polarização Y, sinal descriptografado e recuperado na (e) polarização X e na (f) polarização Y.



Fonte: Elaborado pelo autor.

Os espectros em frequência dos sinais propagados pela primeira rota são mostrados na Figura 20, enquanto os espectros em frequência dos sinais para a propagação pela segunda rota são mostrados na Figura 21. Na Figura 20(a) e Figura 20(b), são apresentados os espectros dos sinais sinalizados em QPSK, gerados sem aplicação da

criptografia e sem terem passado pelo RCF. Na Figura 21(a) e Figura 21(b), são mostrados os espectros dos sinais sinalizados em 16QAM, também gerados sem criptografia e sem terem passado pelo filtro RCF.

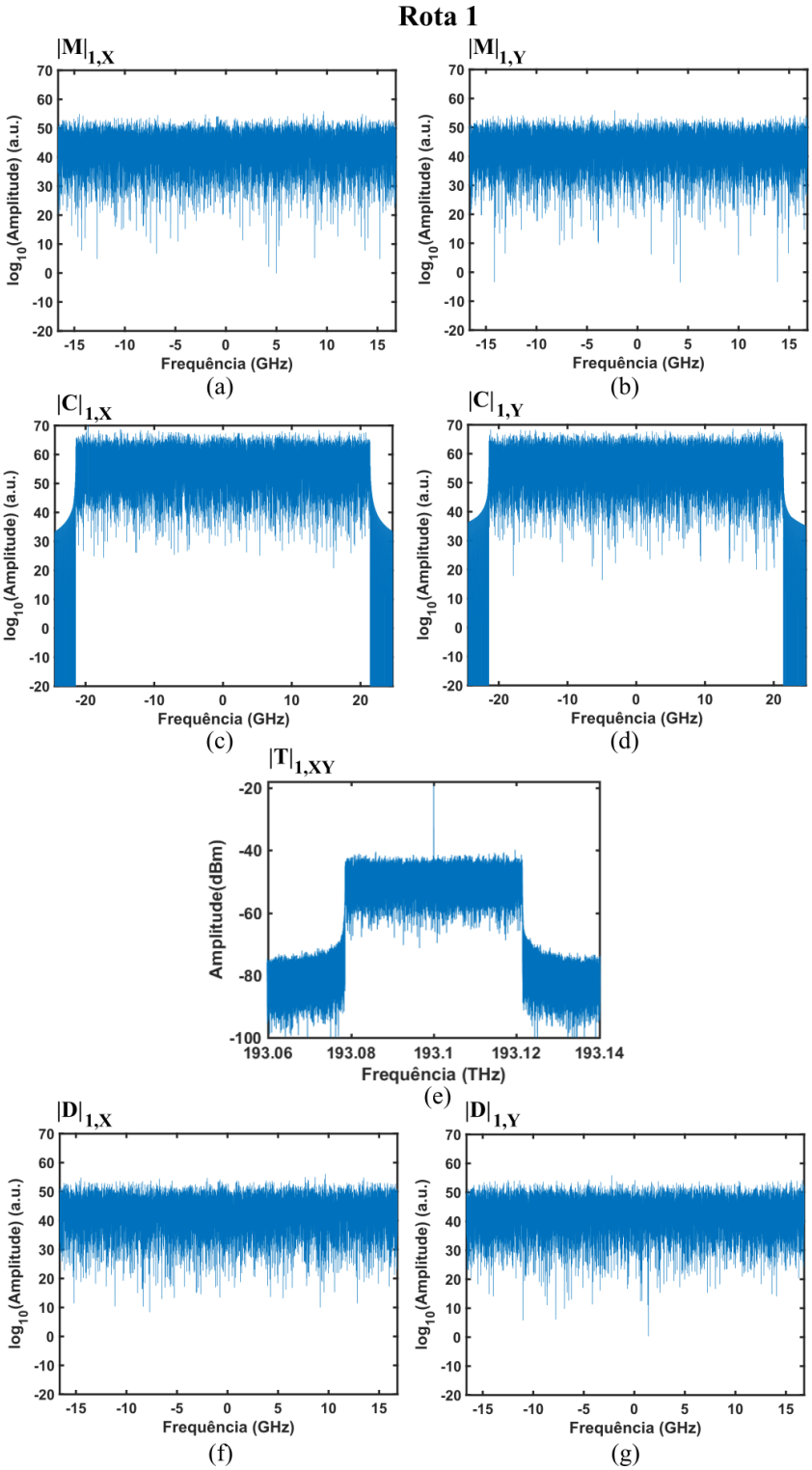
A largura de banda, a taxa de símbolos e o número de símbolos dos sinais referentes aos espectros da Figura 20(a) e Figura 20(b) são menores em comparação aos espectros dos sinais 16QAM e propagados pela segunda rota (Figura 21(a) e Figura 21(b)). Além disso, as amplitudes dos espectros para os sinais QPSK diferem das dos sinais 16QAM, uma vez que as amplitudes geradas para o sinal QPSK são menores, com valores de 1 e -1.

Na Figura 20(c), Figura 20(d), Figura 21(c) e Figura 21(d), são mostrados os espectros dos sinais já passados pelo RCF, criptografados e com largura de banda, taxa de transmissão de símbolo e número de símbolos iguais. Os espectros dos sinais de dupla polarização propagados pela primeira e segunda rotas são mostrados na Figura 20(e) e Figura 21(e), respectivamente. Na Figura 20(f), Figura 20(g), Figura 21(f) e Figura 21(g), são mostrados os espectros correspondentes aos sinais descriptografados e recuperados, com a largura de banda, taxa de transmissão de símbolo e número de símbolos retornados aos valores originais.

Na Figura 22, é apresentado o resultado obtido referente à propagação de dois sinais de dupla polarização pela TON por meio de duas rotas. A nomenclatura das siglas utilizadas na legenda da figura é a mesma adotada para o resultado obtido na Seção 3.1. O sinal de dupla polarização propagado pela primeira rota, como destacado na figura, possui ambas as polarizações com modulação QPSK, enquanto o sinal propagado pela segunda rota possui ambas as polarizações com modulação em 16QAM.

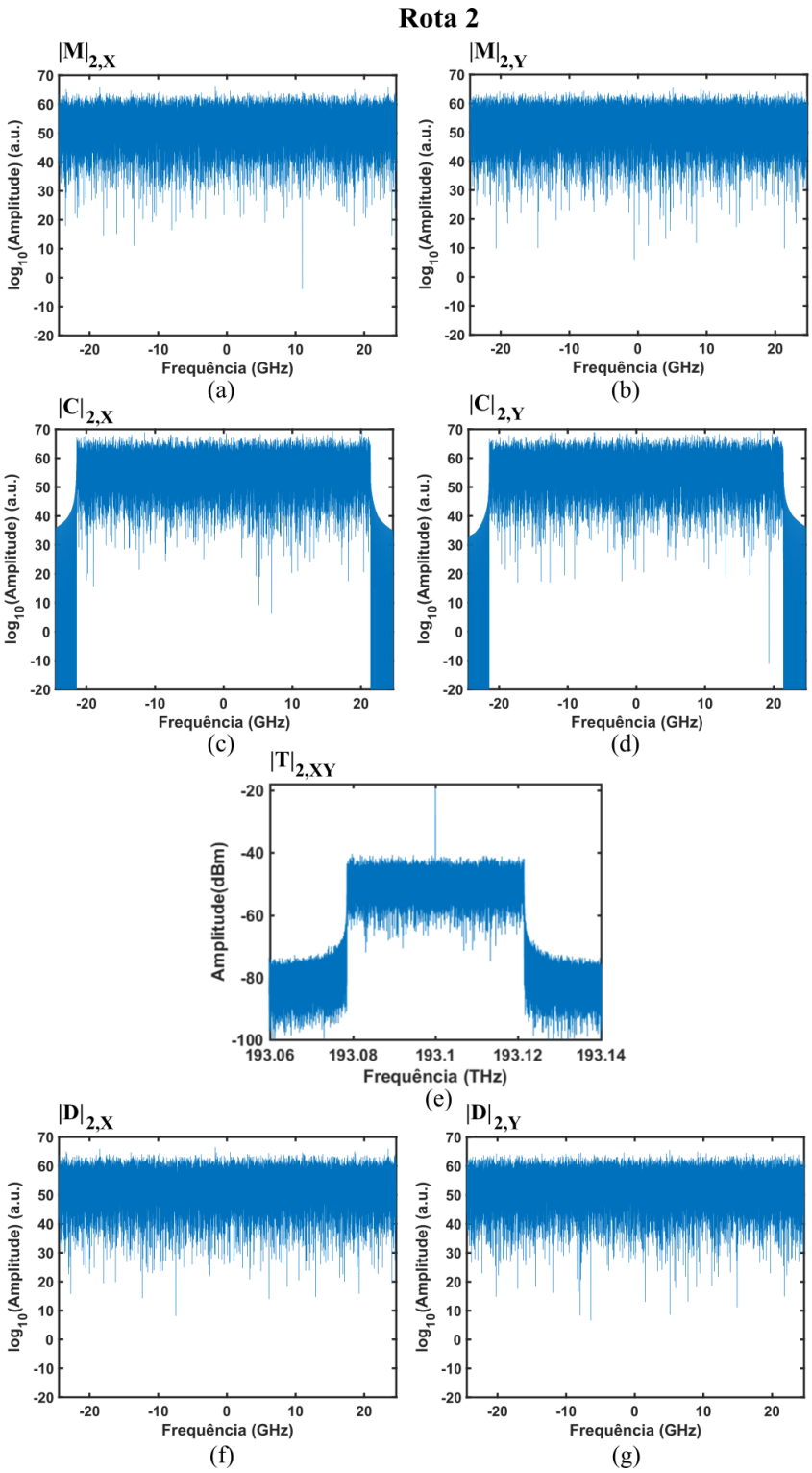
Na Figura 22, as curvas referentes à primeira rota possuíram um comprimento de enlace de fibra óptica de 0 até 1260 km, enquanto as curvas referentes à segunda rota tiveram o comprimento de enlace de fibra óptica fixado em 420 km. As constelações dos sinais descriptografados e recuperados na polarização X, correspondentes à primeira e à segunda rota, estão indicadas em 140 e 1190 km. As constelações mostradas na Figura 22 consideram apenas a polarização X do sinal, exemplificando a qualidade dos sinais descriptografados e recuperados, além de destacar a utilização de diferentes modulações. As constelações dos sinais criptografados na polarização X para a primeira e a segunda rota também são indicadas e mostradas na figura.

Figura 20 - Espectros de amplitude obtidos referentes a primeira rota de propagação correspondendo ao sinal gerado inicialmente na (a) polarização X e na (b) polarização Y, sinal criptografado na (c) polarização X e na (d) polarização Y, (e) sinal criptografado e transmitido contendo as polarizações X e Y, sinal descriptografado e recuperado na (f) polarização X e na (g) polarização Y.



Fonte: Elaborado pelo autor.

Figura 21 - Espectros de amplitude obtidos referentes a segunda rota de propagação correspondentes ao sinal gerado inicialmente na (a) polarização X e na (b) polarização Y, sinal criptografado na (c) polarização X e na (d) polarização Y, (e) sinal criptografado e transmitido contendo as polarizações X e Y, sinal descriptografado e recuperado na (f) polarização X e na (g) polarização Y.



Fonte: Elaborado pelo autor.

No resultado obtido na Figura 22, percebe-se que os sinais criptografados com SPE-SS-Scr-DSP apresentam valores de BER muito próximos até 350 km e se diferenciam a partir desse comprimento. Esse resultado difere dos obtidos anteriormente nos estudos realizados em Abbade (ABBADE, NOGUEIRA, *et al.*, 2020) e Pereira (PEREIRA, NOGUEIRA, *et al.*, 2024), que mostraram valores de BER semelhantes para sinais modulados em 16QAM, criptografados e descriptografados após propagação pela TON em diferentes rotas.

A utilização de diferentes modulações em conjunto com as técnicas de criptografia mostrou uma influência mútua entre os sinais 16QAM e QPSK. Os sinais criptografados e descriptografados em QPSK (SCD_1) mostraram um desempenho inferior em comparação aos sinais QPSK sem criptografia (SSC_1). Por outro lado, os sinais criptografados e descriptografados em 16QAM (SCD_2) mostraram um desempenho superior até o comprimento de fibra óptica de 630 km, mas inferior após esse comprimento em comparação aos sinais 16QAM sem criptografia (SSC_2).

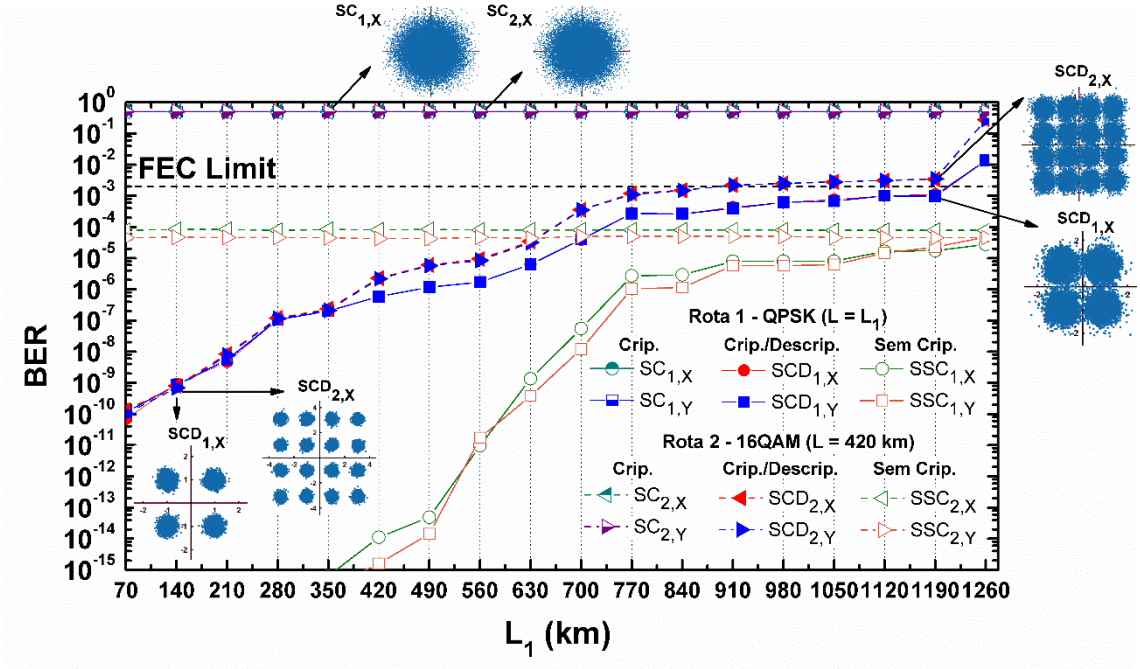
Comparando o resultado obtido e mostrado na Figura 22 com os resultados dos estudos de Abbade (ABBADE, NOGUEIRA, *et al.*, 2020), Pereira (PEREIRA, NOGUEIRA, *et al.*, 2024) e o resultado da Seção 3.1, as curvas referentes ao sinal criptografado e descriptografado propagado pela primeira rota (SCD_1) atingiram um comprimento de enlace de fibra óptica maior, de 910 km, próximo ao limite da FEC. Em contrapartida, as curvas do sinal criptografado e descriptografado propagado pela segunda rota (SCD_2) alcançaram um comprimento de enlace de fibra óptica ainda maior, de 1190 km.

Na Figura 22, observa-se que, após o comprimento de 1190 km, o SCD_1 sofre um aumento considerável no valor da BER. Consequentemente, o SCD_2, que é influenciado pelo comportamento do SCD_1, também sofre um aumento significativo nos valores de BER. Esse resultado é provocado pela utilização da técnica de criptografia SS-DSP, que embaralha as componentes espectrais entre as polarizações dos sinais propagados por ambas as rotas.

A técnica SPE-SS-Ssrc-DSP utilizando DK, quando combinada com técnica de taxas de transmissão distintas, aumenta significativamente a segurança dos sinais propagados por duas rotas. O valor de BER obtido para os sinais criptografados é de aproximadamente 0,5, o que torna difícil a recuperação das informações transmitidas nos

sinais propagados pela TON. Caso haja um intruso na rede, será necessário, além de distinguir as componentes espectrais falsas daquelas que contêm informações e realizar a descriptografia correspondente à técnica de criptografia utilizada, obter os dois sinais propagados pelas duas rotas para que seja possível realizar a descriptografia de acordo com a técnica SS-DSP.

Figura 22 - Gráfico dos valores da BER dado um comprimento de fibra óptica para dois sinais com dupla polarização criptografados em SPE-SS-Scr-DSP e não criptografados sendo propagados por duas rotas em uma TON.



Fonte: Elaborado pelo autor.

O intruso, para acessar as informações transmitidas pela TON, precisaria seguir três etapas descritas no trabalho de Nogueira (NOGUEIRA, 2019): (i) colocar pontos de derivação em cada rota por onde os sinais são transmitidos; (ii) realizar a comunicação entre estes pontos de derivação, o que requer a conexão a um nó de processamento central, tornando necessária a implantação de uma infraestrutura física paralela e complexa de espionagem em relação à infraestrutura legítima da TON; e, por último, (iii) realizar a descriptografia dos sinais e a remoção das componentes espectrais falsas para obtenção das informações que estão sendo transmitidas.

A propagação dos sinais gerados com taxas de transmissão distintas e sinalizações diferentes também possibilitaria a utilização mais flexível e eficiente do espectro, atendendo ao requisito da EON para suprir as altas taxas de transmissões de dados

(NOGUEIRA, 2022). O resultado obtido neste trabalho, mostrado na Figura 22, validou, em simulação, a técnica desenvolvida no estudo de Nogueira (NOGUEIRA, 2022), aplicada a um cenário de comunicação óptica com detecção coerente. Diante dos resultados promissores obtidos, sugere-se a aplicação das técnicas propostas em um ambiente físico de rede de comunicação, a fim de validar sua eficácia em condições operacionais.

4. CONSIDERAÇÕES FINAIS

Os principais tópicos dos fundamentos da criptografia, incluindo a criptografia de dados e na camada física, com destaque para a importância da segurança nos meios de comunicação, foram mencionados e referenciados neste trabalho. A principal proposta deste trabalho de desenvolver um sistema de comunicação óptica em ambiente computacional para avaliação das técnicas de criptografias SPE-SS-Scr-DSP, utilizando DK, aplicadas a sinais de dupla polarização geradas com taxas de transmissão e sinalizações diferentes foi realizada. As melhorias e adaptações foram realizadas no *software* KryptosSJ desenvolvido em Matlab®, e o sistema de comunicação óptico com detecção coerente foi desenvolvido no *software* VPITransmissorMaker™.

O primeiro resultado deste trabalho conclui que a aplicação das técnicas de criptografias, utilizando DK, ao sinal 16QAM de dupla polarização e gerado com diferentes taxas de transmissão de símbolos, propagado por apenas uma rota, não ocasionaram penalidades significativas. Na verdade, obteve-se o mesmo alcance de 700 km de comprimento de enlace de fibra óptica em comparação ao sinal transmitido sem criptografia. No segundo resultado, foram transmitidos dois sinais de dupla polarização por rotas distintas, ambos criptografados utilizando a técnica SPE-SS-Scr-DSP em conjunto com DK e com configurações de taxa de transmissão e sinalização diferentes. O sinal modulado em QPSK foi propagado por uma rota com comprimento variável, enquanto o sinal modulado em 16QAM foi transmitido por uma rota fixa de 420 km. Os resultados indicaram que, após serem descriptografados e recuperados, os sinais atingiram um alcance de aproximadamente 910 km, próximo ao limite FEC. Esse desempenho superior pode ser atribuído ao embaralhamento das componentes espectrais dos sinais com diferentes modulações propagados por rotas distintas, proporcionando maior segurança e alcance em comparação ao primeiro resultado.

Os resultados obtidos neste trabalho demonstraram, portanto, uma boa viabilidade das técnicas estudadas para aplicações em sistemas de comunicação óptica. Sugere-se, para as próximas etapas, validar a eficácia dessas técnicas em condições operacionais. Essa validação prática permitirá avaliar o potencial comercial dessas soluções em diversos setores, como bancos, operadoras de telecomunicações e centros de dados, que demandam níveis cada vez mais elevados de segurança da informação, além de oferecer uma alternativa para redes flexíveis.

REFERÊNCIAS

ABBADE, A. L. D. R.; CAPUTO, M. R. C. Aplicação do OTDR na Análise de Problemas de Atenuação em Fibras Ópticas: Estudo de Casos. **Revista Científica Periódica - Telecomunicações**, 5, n. 2, 2002. 25-33.

ABBADE, M. L. F. et al. All-optical cryptography through spectral amplitude and delay encoding. **Journal of Microwaves, Optoeletronics and Electromagnetic Applications**, v. 12, n. 2, p. 376-397, Dezembro 2013. FabUNIFESP (SciELO). Disponível em: http://dx.doi.org/10.1590/s2179-10742013000200011.

ABBADE, M. L. F. et al. **All-optic phase and delay spectral encoding of signals with adcanced modulation formats**. 16th International Conference on Transparent Optical Networks (ICTON). Graz: IEEE. 2014. DOI: http://dx.doi.org/10.1109/icton.2014.6876372.

ABBADE, M. L. F. et al. **All-optical cryptography of M-QAM formats by using two-dimensional spectrally sliced keys**. The Optical Society. [S.l.]: [s.n.]. 2015. p. 4359-4365. DOI: http://dx.doi.org/10.1364/ao.54.004359.

ABBADE, M. L. F. et al. DSP - Based Multi-Channel Spectral Shuffling Applied to Optical Networks. **IEEE Photonics Technology Letters**, São João da Boa Vista, v. 32, n. 3, p. 154-157, 1 Fevereiro 2020. Disponivel em: <10.1109/LPT.2019.2962837>.

ABBADE, M. L. F. et al. DSP - Based Multi-Channel Spectral Shuffling Applied to Optical Networks. **IEEE Photonics Technology Letters**, São João da Boa Vista, v. 32, n. 3, p. 154-157, 1 Fevereiro 2020. DOI: 10.1109/LPT.2019.2962837.

ABBADE, M. L. F. et al. DSP - Based Multi-Channel Spectral Shuffling Applied to Optical Networks. **IEEE Photonics Technology Letters**, São João da Boa Vista, v. 32, n. 3, p. 154-157, 1 Fevereiro 2020. Disponivel em: <10.1109/LPT.2019.2962837>.

ABBADE, M. L. F. et al. **Signal Encryption Opportunities for Photonic Networks**. OSA Advanced Photonics Congress (IPR, NP, NOMA, Networks, PVLED, PSC, SPPCom, SOF), L. Caspani, A. Tauke-Pedretti, F. Leo, and B. Yang, eds., OSA Technical Digest (Optical Society of America). [S.l.]: OSA Advanced Photonics Congress (AP) (IPR, NP, NOMA, Networks, PVLED, PSC, SPPCom, SOF). 2020. DOI: https://doi.org/10.1364/NETWORKS.2020.NeTu1B.2.

ABBADE, M. L. F. et al. Discrete Spectral Encryption of Single-Carrier Signals With Pseudo Random Dynamic Keys. **IEEE Transactions on Information Forensics and Security**, v. 19, p. 4914-4929, 2024. DOI: 10.1109/TIFS.2024.3390995.

ADVISOR, C. Brasil lidera ranking de vazamento de dados em 2021. 3 de fevereiro de 2022, 2022. Disponivel em: <https://www.cisoadvisor.com.br/brasil-lidera-ranking-de-vazamento-de-dados-em-2021/#:~:text=Com%202%2C8%20bilh%C3%B5es%20de,a%20riscos%20digitais%20na%20internet>. Acesso em: 30 Novembro 2023.

AGRAWAL, G. P. **Sistema de Comunicação por Fibra Óptica**. 4ª. ed. Rio de Janeiro: Elsevier, 2014.

APARECIDO DE PAULA, R. et al. Projeto de um modulador Mach-Zehnder de silício via aprendizado profundo e algoritmos evolutivos. **Sci Rep 13**, n. 14662, p. 12, Setembro 2023.

ARGYRIS, A. et al. Chaos-based communications at high bit rates using commercial fibre-optic links. **Nature**, v. 438, p. 343-346, 2005. DOI: https://doi.org/10.1038/nature04275.

ASSIS, K. D. R.; SANTOS, C. C. **Planejamento e Segurança em Redes Ópticas:** Uma Estratégia para Minimizar os Efeitos do Ataque Jamming. XLIII Simpósio Brasileiro de Pesquisa Operacional. Ubatuba, SP: [s.n.]. 2011. p. 15-18.

BANDEIRA, A. P. V. **Classificação, quantificação e dinâmica do Emaranhamento**. Universidade Federal de Campina Grande, Centro de Ciências e Tecnologias. Campina Grande, p. 79. 2013.

BARKAN, E.; BIHAM, E.; KELLER, N. **Instant ciphertext-only cryptanalysis of gsm encrypted communication.** Annual international cryptology conference. Springer: [s.n.]. 2003. p. 600-616.

BOARON, A. et al. Secure Quantum Key Distribution over 421 km of Optical Fiber. **Phys. Rev. Lett.**, v. 121, n. 19, p. 190502, Nov. 2018. DOI: 10.1103/PhysRevLett.121.190502.

BOBADILLHA, L. D. B. **Criptografia Óptica Mediante Fatiamento e Embaralhamento Espectrais**. Universidade Estadual Paulista "Júlio de Mesquita Filho" (UNESP). São João da Boa Vista, p. 1-36. 2018. Trabalho de Conclusão de Curso de graduação.

BRAGAGNOLLE, A. et al. **All-Optical Spectral Shuffling of Signals Traveling throug Different Optical Routes**. 2019 21st International Conference on Transparent Optical Networks (ICTON). [S.l.]: [s.n.]. 2019. p. 1-4. DOI: 10.1109/ICTON.2019.8840243.

CAMARGO, A. L. P. Simulação do protocolo BB84 de criptografia quântica utilizando um feixe laser intenso. **Revista Brasileira de Ensino de Física**, v. 39, 2017. DOI: https://doi.org/10.1590/1806-9126-RBEF-2016-0149.

CHEN, Y.; ZHANG, Q.; CHEN, T. An integrated space-to-ground quantum communication network over 4,600 kilometres. **Nature 589**, 2021. 214–219. DOI: https://doi.org/10.1038/s41586-020-03093-8.

CHENG, X. C. et al. Security enhancement of double-random phase encryption by amplitude modulation. **Opt. Lett.**, v. 33, n. 14, p. 1575-1577, 2008.

CISCO. **Cisco Annual Internet Report (2018 - 2023)**. The Cisco Annual Internet Report. [S.l.], p. 35. 2020.

CISCO VISUAL NETWORKING INDEX. **The Zettabyte Era:Trends and Analysis**. CISCO. [S.l.], p. 32. 2017.

COLET, P.; ROY, R. Digital communication with synchronized chaotic lasers. **Opt. Lett. 19**, p. 2056-2058, 1994.

COLLINS, L. Optical Network Security. In: KAUFMANN, M. **Computer and Information Security Handbook**. 2nd. ed. [S.l.]: ELSEVIER, 2013. Cap. 19, p. 363-370.

CORNEJO, J.; TOCNAYE, J. L. D. B. Non-invansive WDM channel scrambling for secure high data rate optical transmissions. **Photon Management III**, v. 6994, p. 127-131, 2008. In: Sheridan, J. T.; WYROWSKI, F. (Ed).

COZZENS, M.; MILLER, S. J. **The Mathematics of Encryption An Elementary Introduction**. [S.l.]: American Mathematical Soc., v. 29, 2013.

CUOMO, M.; OPPENHEIM, A. V.; STROGATZ, S. H. Synchronization of Lorenz-based chaotic circuits with applications to communications. **IEEE Trans. Circuits Sys. II 40**, p. 626-633, 1993.

DAEMEN, J.; RIJMEN, V. **AES Proposal: Rijndael**. [S.l.], p. 45. 1999. Disponível em: https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.197-upd1.pdf.

DE ARAÚJO, E. J. **Criptografia: dos rudimentos à atualidade**. UFRJ. Rio de Janeiro, p. 76. 2018. Dissertação de Mestrado.

ETERNAL. Product Catalogue. Disponivel em: <https://esfiberscopes.com/product-category/handheld-fiber-optic-inspection-probes/?gclid=Cj0KCQiAnuGNBhCPARIsACbnLzqQWZ4-iBm2Mx5xRPsNHTJybvVvyL9BZ3H4sDk4mdSWSsFeH8N9KTcaAkU7EALw_wcB>. Acesso em: 10 Dezembro 2021.

EXFO. FIP-500 fiber inspection scope. Disponivel em: <https://www.exfo.com/en/products/field-network-testing/fiber-inspection/fip-500/?gclid=Cj0KCQiAnuGNBhCPARIsACbnLzoZ6kS5iZHVoN7vupQWfqrWM8xGkeaV9rmd7U5vGubfPvsVaMRmIKAaArrrEALw_wcB>. Acesso em: 10 Dezembro 2021.

FAN, L. et al. Real-time observation and control of optical chaos, v. 279, p. 1198-1200, 1998. Disponivel em: </doi/10.1126/sciadv.abc8448>. DOI: /doi/10.1126/sciadv.abc8448.

FANG, X.; ZENG, P.; LIU, H. Implementation of quantum key distribution surpassing the linear rate-transmittance bound. **Nature Photonics**, p. 422-425, July 2020. DOI: https://doi.org/10.1038/s41566-020-0599-8.

FARIAS, G. F. **5G - Redes de comunicações móveis de quinta geração: evolução, tecnologia, aplicações e mercado**. Engenharia Elétrica da Universidade do Sul de Santa Catarina (UNISUL). Palhoça, p. 88. 2019. Trabalho de Conclusão de Curso apresentado no curso de graduação.

FAY, R. Introducing the counter mode of operation to Compressed Sensing based encryption. **Information Processing Letters**, v. 116, n. 4, p. 279-283, 2016. DOI: https://doi.org/10.1016/j.ipl.2015.11.010.

FERREIRA, V. L. R. P.; AMARO, S. C.; PINHEIRO, L. G. **Distribuição de chaves quânticas com o protocolo BB84 nos simuladores quânticos da IBM**. Faculdade de

Tecnologia de Americana "Ministro Ralph Biasi". Americana, p. 22. 2023. Trabalhos de Conclusão de Curso.

FIPS. **Advanced Encryption Standard (AES)**. National Institute of Standards and Technology. [S.l.]. 2001. Federal Information Processing Standards Publication. DOI: https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.197-upd1.

FIPS, N. 1. **Announcing the Advanced Encryption Standard.** National Institute of Standards and Technology (NIST). [S.l.], p. 1-47. 2001.

GALLAGHER, J. N. C. Discrete Spectral Phase Coding. **IEEE Transactions on Information Theory**, September 1976. 622-624.

GENG, C. et al. **Multi-fold physical layer data encryption using chaotic frequency hopping**. 2018 20th International Conference on Transparent Optical Networks (ICTON). [S.l.]: IEEE. 2018. p. 1-4.

GERSTEL, O. Elastic optical networking: a new dawn for the optical layer. **IEEE Communications Magazine**, v. 50, p. 12-20, 9 Fevereiro 2012. DOI:http://dx.doi.org/10.1109/mcom.2012.6146481.

GERSTEL, O. Elastic optical networking: a new dawn for the optical layer. **IEEE Communications Magazine**, v. 50, p. 12-20, 9 Fevereiro 2012. Disponivel em: <http://dx.doi.org/10.1109/mcom.2012.6146481>.

GILMORE, J. **EFF builds DES cracker that proves that data encryption standard is insecure.** [S.l.]. 1998. [S.l.]: EFF press release.

HU, X. et al. Chaos-based partial transmit sequence technique for physical layer security in ofdm-pon. **IEEE Photonics Technology**, 27, n. 23, 2015. 2429-2432.

IBGE. Censo 2022 indica que o Brasil totaliza 203 milhões de habitantes. **Serviços e Informações do Brasil**, 2023. Disponivel em: <https://www.gov.br/pt-br/noticias/financas-impostos-e-gestao-publica/2023/06/censo-2022-indica-que-o-brasil-totaliza-203-milhoes-de-habitantes>. Acesso em: 22 Agosto 2024.

IDQ REDEFINING SECURITY. **Quantum-Safe Security White Paper - Understangin Quantum Cryptografy**. IDQ Redefining Security. [S.l.], p. 16. 2020.

IOS. International Organization for Standardization. **ISO/IEC 7498:** Information technology - Open Systems Interconnection - Basic Reference Model, 1984. Disponivel em: <https://www.iso.org/obp/ui/#iso:std:20269:en>. Acesso em: 1 Dezembro 2021.

ITU. Statistics. **International Telecommuncation Union**, 2023. Disponivel em: <https://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx>. Acesso em: 21 Agosto 2024.

JENKINS, F. A.; WHITE, H. E. **Fundamentals Of Optics**. 4. ed. New York, Caracas, New Delhi: McGraw-Hill Primis Custom Publishing, 2001.

JUNIOR, J. A. B. **Especificação estatística da dispersão dos modos de polarização em enlaces ópticos**. Pontifícia Universidade Católica do Rio de Janeiro. Rio de Janeiro,

p. 62. 2003. Dissertação de Mestrado - Departamento de Engenharia Elétrica, Pontifícia Universidade Católica do Rio de Janeiro.

KARTALOPOULOS, S. V. Quantum Cryptography For Secure Optical Networks. **IEEE International Conference on Communications**, p. 1311-1316, 2007. DOI: 10.1109/ICC.2007.221.

KATZ, J.; LINDELL, Y. **Introduction to modern cryptografy**. 2nd. ed. Boca Raton: Chapman & Hall/CRC, 2014.

KE, J. et al. Key technologies in chaotic optical communications Frontiers of Optoelectronics. **Springer**, v. 9, n. 3, p. 508-517, 2016.

KIM, K. S. Ultrareliable and Low-Latency Communication Techniques for Tactile Internet Services. **Proceedings of the IEEE**, 107, Feb. 2019. 376-393. DOI: 10.1109/JPROC.2018.2868995.

KITAYAMA, K.-I. Security in Photonic Networks: Threats and Security Enhancement. **Journal of Lightwave Technology**, Piscataway, v. 29, p. 3210-3222, Novembro 2011. DOI: http://dx.doi.org/10.1109/jlt.2011.2166248.

KOBLITZ, N. **A course in number theory and cryptography**. 2nd. ed. [S.l.]: Springer Science & Business Media, v. 114, 1994.

LATHI, B. P.; DING, Z. **Sistemas de Comunicações Analógicos e Digitais Modernos**. 4ª. ed. Rio de Janeiro: LTC, 2012. Tradução por J. R. Souza e revisão técnica de José Alexandre Nalon.

LIAO, S.; CAI, W.; LIU, W. Satellite-to-ground quantum key distribuition. **Nature**, v. 549, p. 43-47, 9 August 2017. DOI: https://doi.org/10.1038/nature23655.

LIAO, S.; CAI, W.; LIU, W. Satellite-to-ground quantum key distribuition. **Nature**, v. 549, p. 43-47, 9 August 2017.

LU, Y.; MEIER, W.; VAUDENAY, S. **The conditional correlation attack:** A practical attack on bluetooth encryption. Annual International Cryptology Conference. SPRINGER: [s.n.]. 2005. p. 97-117.

LYDIA, B.; SMAIL, B.; MOHAMED, S. Application of quantum cryptografy in an optical link. **International Conference on Electrical Engineering**, Boumerdes, 2017. Boumerdes: IEEE,2017.

MARQUEZINO, F. L.; HELAYEL-NETO, J. A. **Estudo Introdutório do Protocolo Quântico BB84 para Troca Segura de Chaves**. Centro Brasileiro de Pesquisas Fısicas, Série Monografias. Rio de Janeiro, p. 15. 2003.

MENEZES, A. J. et al. Handbook of applied cryptography, 1996.

NGO, H. H. Dymanic Key Cryptography and Applications. **International Journal of Network Security**, 10, Maio 2010. 161-174.

NOGUEIRA, M. P. **Propagação de sinais ópticos criptografados por meio de embaralhamento espectral**. Universidade Estadual Paulista Júlio de Mesquita Filho -

Câmpus de São João da Boa Vista. São João da Boa Vista, p. 1-41. 2019. Relatório Final de Projeto de Pesquisa desenvolvido com poio da FAPESP.

NOGUEIRA, M. P. **Criptografia física por embaralhamento espectral aplicada a sinais com taxas de transmissão distintas.** Universidade Estadual Paulista "Júlio de Mesquita Filho" (UNESP). São João da Boa Vista, p. 65. 2022.

NOGUEIRA, M. P. et al. **Enhancing Inter-Data Centre Link Security with Spectral Polarisation Shuffling and Phase Encoding**. Bucharest, Romania: 23rd International Conference on Transparent Optical Networks (ICTON). 2023. doi: 10.1109/ICTON59386.2023.10207283.

NOGUEIRA, M. P. et al. **Enhancing Inter-Data Centre Link Security with Spectral Polarisation Shuffling and Phase Encoding**. Bucharest, Romania: 23rd International Conference on Transparent Optical Networks (ICTON). 2023.

NÚCLEO DE INFORMAÇÃO E COORDENAÇÃO DO PONTO BR. 80% dos domicílios brasileiros possuem acesso à internet, aponta pesquisa. **Ministério das Comunicações (GOV)**, 2023. Disponivel em: <https://www.gov.br/mcom/pt-br/noticias/2023/maio/80-dos-domicilios-brasileiros-possuem-acesso-a-internet-aponta-pesquisa>. Acesso em: 22 Agosto 2024.

ODEN, J. et al. Multi-Gbit/s optical phase chaos communications using a time-delayed optoelectronic oscillator with a three-wave interferometer nonlinearity. **Chaos: An Interdisciplinary Journal of Nonlinear Science**, v. 27, n. 11, p. 114311, 2017. ISSN AIP Publishing.

ORUMA, S. O. . P. S. Security Threats to 5G Networks for Social Robots in Public Spaces: A Survey. **IEEE Acess**, v. 11, p. 63205-63237, 2023. DOI: 10.1109/ACCESS.2023.3288338.

PALAIS, J. C. **Fiber Optic Communications**. 5ª. ed. [S.l.]: Pearson, 2004. 456 p.

PANISSON, A. et al. **Segurança em Redes Ópticas:** Tipos de Ataques e Métodos de Detecção. 2ª Escola Regional de Redes de Computadores - ERRC. Porto Alegre: SBC: Anais. 2004. p. 103-108.

PEREIRA, J. P. D. L. C. et al. **Propagation of Optical Signals Encrypted with Spectral Phase Encoding and Signal/Polarisation Shuffling**. 2024 24th International Conference on Transparent Optical Networks (ICTON). Bari, Italy: IEEE. 2024. p. 1-4. DOI: 10.1109/ICTON62926.2024.10647852.

PEY, J. N. A.; NZE, G. D. A.; ALBUQUERQUE, R. D. O. **Analysis of jamming and spoofing cyberattacks on drones**. 17th Iberian Conference on Information Systems and Technologies (CISTI). Madrid, Spain: IEEE. 2022. p. 1-4. DOI: 10.23919/CISTI54924.2022.9820201.

RIGOLIN, G.; RIEZNIK, A. A. Introdução à criptografia quântica. **Revista Brasileira de Ensino de Física**, v. 27, p. 517-526, 2005.

RIJMEN, V.; DAEMEN, J. Advanced Encryption Standard. **Proceedings of Federal Information Processing Standards Publications, National Institute of Standards and Technology**, 26 Novembro 2001. 19-22.

SANTOS, M. O. **Criptografia na camada física baseada em codificação espectral implantada por meio de DSP e aplicada a redes ópticas**. Universidade Estadual Paulista Júlio de Mesquita Filho - Câmpus de São João da Boa Vista. São João da Boa Vista, p. 1-65. 2020. Disponível em: http://hdl.handle.net/11449/192881.

SANTOS, M. O. **Criptografia na camada física baseada em codificação espectral implantada por meio de DSP e aplicada a redes ópticas**. Universidade Estadual Paulista Júlio de Mesquita Filho - Câmpus de São João da Boa Vista. São João da Boa Vista, p. 1-65. 2020. http://hdl.handle.net/11449/192881.

SCHNEIER, B. **Applied Cryptografy**. [S.l.]: John Wiley & Sons, 1996.

SHAFI, G.; SILVIO, M. **Probabilistic encryption & how to play mental poker keeping secret all partial information**. [S.l.]: [s.n.]. 1982.

SHANNON, C. E. Communication Theory of Secrecy Systems. **BELLTJ**, v. 28, p. 656-715, 1949.

SHANNON, C. E. Communication Theory of Secrecy Systems. **Bell System Technical**, v. 28-4, p. 656–715, 1949.

SIDDIQI, M. A.; J., J. H. Y. E. 5G Ultra-Reliable Low-Latency Communication Implementation Challenges and Operational Issues with IoT Devices". Electronics. **IEEE Acess**, v. 8, p. 981, November 2019. DOI: 103390/electronics8090981.

SOMA, D. 16-Peta-bit/s Dense SDM/WDM Transmission over 6-Mode 19-Core Fiber across the C+L Band. **Journal of Lightwave Technology**, Piscataway, 30 Janeiro 2018. 1-8. Disponivel em: <http://dx.doi.org/10.1109/jlt.2018.2799380>.

SOUZA, W. S. **Adaptação de criptografia espectral ao paradigma do "Advanced Encryption Standard"**. Dissertação (mestrado) - Universidade Estadual Paulista (Unesp), Câmpus de São João da Boa Vista. São João da Boa Vista, p. 95. 2021.

SOUZA, W. S. E. A. **Adaptação de Criptografia Espectral ao Paradigma do Advanced Encryption Standard**. Universidade Estadual Paulista "Júlio de Mesquita Filho" (UNESP) Câmpus de São João da Boa Vista. São João da Boa Vista, p. 1-65. 2022.

SOUZA, W. S. et al. **Spectral Shuffling with Phase Encoding and Dynamic Keys Applied to Transparent Optical Network Signals**. 2020 22nd International Conference on Transparent Optical Networks (ICTON). [S.l.]: [s.n.]. 2020. p. 1-4. DOI: 10.1109/ICTON51198.2020.9203374.

STALLINGS, W. **Criptografia e segurança de redes princípios e práticas**. 6ª ed. ed. São Paulo: Pearson Education do Brasil, 2014.

STINSON, D. R.; PATERSON, M. **Cryptography:** theory and practice. [S.l.]: CRC press, 2018.

SUCHAT, S.; PAIBOON, S.; YUPAPIN, P. P. An experiment of optical encryption technique with quantum security for mobile phone up-link converter. **IEEE International Conference on Industria Techology**, v. 2, p. 1245-1248, 2002. DOI:10.1109/ICIT.2002.1189353.

SULTAN, A. et al. Chaotic constellation mapping for physical-layer data encryption in OFDM-PON. **IEEE Photonics Technology Letters, IEEE**, 30, 2018. 339-342.

SURFSHARK. Global data breach statistics, 2024. Disponivel em: <https://surfshark.com/research/data-breach-monitoring>. Acesso em: 21 Agosto 2024.

TANENBAUM, A. S.; WETHERALL, D. J. **Computer networks Pearson**. [S.l.]: [s.n.], 2010.

TELEGEOGRAFY. Submarine Cable Map, 2024. Disponivel em: <https://www.submarinecablemap.com/>. Acesso em: 18 Setembro 2024.

TYCHOPOULOS, A.; KOUFOPAYLOU, O.; TOMKOS, I. FEC in optical communications - A tutorial overview on the evolution of archietectures and the future prospects of outband and inband FEC for optical communications, v. 22, n. 6, p. 79-86, Nov.-Dec. 2006. DOI: 10.1109/MCD.2006.307281.

TYCHOPOULOS, A.; KOUFOPAYLOU, O.; TOMKOS, I. FEC in optical communications - A tutorial overview on the evolution of archietectures and the future prospects of outband and inband FEC for optical communications, v. 22, n. 6, p. 79-86, Nov.-Dec. 2006.

WILKINSON, L. Increasing Optical Fiber Capacity and Channel Data Rates in Submarine Communication Cables. **Advancing Optics and Photonics Wordwide (OSA)**, 13 Abril 2021. Disponivel em: <https://www.optica.org/en-us/about/newsroom/news_releases/2021/increasing_optical_fiber_capacity_and_channel_data/>. Acesso em: 10 Dezembro 2021.

WU, H.; PRENEEL, B. **Key recovery attack on py and pypy with chosen ivs. eSTREAM, ENCRYPT**. ENCRYPT Stream Cipher Project. Citeseer, p. 2006. 2006.

WU, H.; PRENEEL, B. **Differential-linear attacks against the stream cipher phelix.** International Worshop on Fast Software Encryption. SPRINGER: [s.n.]. 2007. p. 87-100.

YANG, X. et al. Chaotic encryption algorithm against chosen-plaintext attacks in optical ofdm transmission. **IEEE Photonics Technology Letters**, 28, n. 22, 2016. 2499-2502.

YIN, J. . L. Y. . L. S. Entanglement-based secure quantum cryptography over 1,120 kilometres. **Nature 582**, 2020. 501-505. DOI: https://doi.org/10.1038/s41586-020-2401-y.

ZAIDI, S. M. H. **Quantum Internet:** A Revolutionary Disruption. IEEE 19th International Conference on Smart Communities: Improving Quality of Life Using ICT, IoT and AI, HONET 2022. [S.l.]: IEEE. 2022. p. 146-150.

ZHANG, G. et al. A Survey on OFDM-Based Elastic Core Optical Networking. **IEEE Communications Surveys & Tutorials**, v. 15, p. 65-87, 2013. DOI: 10.1109/SURV.2012.010912.00123.

ZHANG, G. et al. A Survey on OFDM-Based Elastic Core Optical Networking. **IEEE Communications Surveys & Tutorials**, v. 15, p. 65-87, 2013. Disponivel em: <10.1109/SURV.2012.010912.00123>.

ZHANG, L. et al. Secure OFDM-PON Based on Chaos Scrambling. **IEEE Photonics Technology Letters**, v. 23, n. 14, p. 998-1000, July 2011. DOI: 10.1109/LPT.2011.2149512.

ZHANG, Q. et al. Megabits secure key rate quantum key distribution. **New Journal of Physics**, v. 11, n. 4, p. 045010, 2009. ISSN IOP Publishing.

ANEXO A – Técnica de taxas de transmissão distintas

Neste anexo é descrito com mais detalhes as etapas realizadas no código para aplicação da técnica de taxa de transmissão distintas, possibilitando que sinais criptografados com embaralhamento espectral intercanal (SS-DSP) possam ser transmitidos e recuperados. Os sinais são gerados com os parâmetros de taxas de transmissão de símbolos e largura de banda distintas e transmitidos pelo canal com taxas de transmissão e com largura de banda iguais.

O sinal que tem a maior taxa de transmissão de símbolo e o maior número de amostras não há necessidade de ser alterado para ser transmitido pelo canal. Porém, o sinal que possui menor taxa de transmissão de símbolo e menor número de amostras há a necessidade de realizar alterações para que assuma, durante a transmissão, o mesmo valor da taxa de transmissão de símbolos e, consequentemente o mesmo número de símbolos e amostras.

Por exemplo, a função "Mapeador" gera os dois sinais. Considerando o sinal $m_1[n]$ com menor número de amostras e menor taxa de transmissão e o $m_2[n]$ com maior número de amostras e maior taxa de transmissão. No sinal $m_1[n]$ são adicionadas amplitudes falsas na função chamada de "Adição de Amplitudes Falsas". A técnica é aplicada seguindo as seguintes etapas:

1. Calcular o número de bits necessários para que sejam gerados e, posteriormente, acrescentados ao sinal $m_1[n]$ de forma que fique do mesmo tamanho (com mesmo número de amostras) que o sinal $m_2[n]$:

$$n_{bits\_falsos} = n_{bits\_2} - n_{bits\_1} \tag{9}$$

   Sendo n_{bits_falsos} o número de bits que serão acrescentados ao sinal $m_1[n]$, n_{bits_2} o número de bits do sinal $m_2[n]$ e n_{bits_1} o número de bits do sinal $m_1[n]$.

2. Gerar uma palavra PRBS a partir do número de n_{bits_falsos} calculados na etapa 1.
3. Mapear os bits em símbolos (seja 2 ou 4 bits por símbolo) associados aos eixos I e Q de acordo com o tipo de modulação do sinal $m_1[n]$.
4. Converter os bits em amplitudes de acordo com o tipo de modulação. Exemplo considerando um vetor de 4 amplitudes falsas necessárias para acrescentar ao sinal $m_1[n]$. As amplitudes falsas são geradas para os eixos I e Q do sinal $m_1[n]$:
   a. Amplitudes Falsas I = [1 1 -3 -1]

b. Amplitudes Falsas Q = [3 1 3 -1]

5. Gerar chaves com posições onde as amplitudes falsas serão acrescentadas no sinal $m_1[n]$. Exemplo considerando um vetor de 4 posições:
   a. As amplitudes falsas são geradas para os eixos I e Q do sinal $m_1[n]$:
      a. Posições das Amplitudes Falsas I = [2 5 7 10]
      b. Posições das Amplitudes Falsas Q = [1 4 6 9]
6. Dividir o sinal $m_1[n]$ no eixo I e eixo Q e amostrar os pontos. As amplitudes falsas são adicionadas a partir das posições contidas no vetor "Posições das Amplitudes Falsas" nos eixos I e Q do sinal $m_1[n]$. A parte real e imaginária do sinal $m_1[n]$ com as amplitudes falsas são chamadas de $m_{1_{falso\_I}}[n]$ e $m_{1_{falso\_Q}}[n]$, respectivamente. Os demais valores de amplitudes já contidos no sinal $m_1[n]$ serão deslocados para a posição seguinte assim que acrescentado a amplitude falsa. Considerando o sinal $m_1[n]$ de tamanho 10 amostras com modulação em 16QAM e sendo necessário acrescentar 4 amplitudes falsas nos eixos I e Q:
   a. Gera-se o sinal $m_1[n]$:
      i. $m_1[n]$ = [1+3i 0 3-1i 0 -1+1i 0 1+3i 0 -3-3i 0 1+1i 0 3-1i 0 3+3i 0 1-1i 0 -3+1i]
   b. Seleciona-se os pontos de amostragem dos eixos I e Q de $m_1[n]$:
      i. $m_{1\_I}[n]$ = [1 3 -1 1 -3 1 3 3 1 -3]
      ii. $m_{1\_Q}[n]$ = [3 -1 1 3 -3 1 -1 3 -1 1]
   c. Gera-se um vetor que contém as posições de onde serão acrescentadas as amplitudes falsas:
      i. Posições das Amplitudes Falsas I = [2 5 7 10]
      ii. Posição das Amplitudes Falsas Q = [1 4 6 9]
   d. Gera-se as amplitudes falsas:
      i. Amplitudes Falsas I = [1 3 -3 -1]
      ii. Amplitudes Falsas Q = [3 1 3 -1]
   e. Acrescenta as amplitudes falsas aos eixos I e Q no sinal $m_1[n]$. Os números em vermelho e sublinhados são as amplitudes falsas adicionadas e os números em azul e não sublinhados são os valores originais, como exemplo:
      i. $m_{1\_I\_falso}[n]$ = [1 1 3 -1 3 1 -3 -3 1 -1 3 3 1 -3]
      ii. $m_{1\_Q\_falso}[n]$ = [3 3 -1 1 1 3 3 -3 -1 1 -1 3 -1 1]

7. As posições originais dos valores de amplitudes dos sinais $m_{1\_I}[n]$ e $m_{1\_Q}[n]$ são armazenadas em uma chave, chamada no diagrama mostrado da Figura 4 de "Chave de Amplitudes Falsas".
8. O mesmo procedimento feito no "Mapeador" é realizado nessa etapa. Os valores de amplitudes são colocados nas posições de amostragem ímpares.
9. Os sinais $m_{1\_I\_falso}[n]$ e $m_{2\_Q\_falso}[n]$ são combinados e é gerado o novo sinal $m_{1\_falso}[n]$:

   $m_{1\_falso}[n]$ = [1+3i 0 1+3i 0 3-1i 0 -1+1i 0 3 + 1i 0 1+3i 0 -3+3i 0 -3-3i 0 +1-1i 0 -1+1i 0 3-1i 0 3+3i 0 1-1i 0 -3+1i]
10. O sinal $m_{1\_falso}[n]$ possui o mesmo tamanho e a mesma taxa de transmissão do sinal $m_2[n]$.
11. O submódulo "Remoção de Amplitudes Falsas" é responsável por selecionar os pontos de amostragem do sinal $m_{1\_falso}[n]$ e é utilizado a "Chave Amplitudes Originais" para extrair do sinal $m_{1\_falso}[n]$ apenas os valores originais que correspondem ao sinal $m_1[n]$ nos eixos I e Q. Posteriormente, os eixos I e Q são combinados e o $m_1[n]$ retorna a ser:

    $m_1[n]$ = [1+3i 0 3-1i 0 -1+1i 0 1+3i 0 -3-3i 0 1+1i 0 3-1i 0 3+3i 0 1-1i 0 -3+1i]
12. Dessa forma, é restaurado o número de amostras, a taxa de transmissão de símbolo originais e a largura de banda do sinal $m_1[n]$.

ANEXO B – Técnica de embaralhamento espectral intercanal

Neste anexo será descrito com mais detalhes as etapas necessárias para realização do embaralhamento espectral intercanal utilizando processamento digital de sinal. Na função “Embaralhador Espectral Intercanal”, é realizado a troca das amostras espectrais por meio das variáveis declaradas em “Parâmetros 1” e “Parâmetros 2”. As etapas para a geração da chave de embaralhamento espectral são:

1. Calcula o número de trocas possíveis entre os n_{ch} sinais utilizando fatorial e armazenar em uma determinada variável “N_p”:
$$N_p = n_{ch}!$$
2. A posição de cada amostra será realocada de acordo com a chave “$K_{shuffled}$”. O cálculo da chave é obtido por meio de uma iteração percorrendo o número de amostras.
3. Na iteração, a primeira parte é responsável por definir uma matriz contendo todas as possibilidades de trocas entre as amostras espectrais chamada de “MP” de acordo com o número de sinais. Por exemplo, caso de 2 sinais, obtém-se a permutação de 2, o que resulta na seguinte matriz:
$$MP = \begin{bmatrix} 1 & 2 \\ 2 & 1 \end{bmatrix},$$
No caso de considerarmos 3 sinais, obtém-se então:
$$MP = \begin{bmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \\ 3 & 2 & 1 \\ 3 & 1 & 2 \\ 2 & 3 & 1 \\ 2 & 1 & 3 \end{bmatrix}$$
4. A segunda parte da iteração é definido um valor aleatório, chamado de L_a, que será utilizado para obter uma linha aleatória da MP. O valor de L_a é obtido a partir do número de possibilidades de trocas definida como N_p em 1.
5. A terceira parte da iteração é selecionado a linha aleatória da matriz MP e, então, essa linha é atribuída a matriz correspondente a chave “$K_{shuffled}$”.
6. A primeira iteração corresponde ao realocamento das posições das primeiras amostras de cada sinal. No caso da primeira iteração, considerando $n_{ch} = 2$ e $L_a = 5$, obtem a chave sendo:
$$K_{shuffled} = [2 \quad 3 \quad 1]$$

Nesse caso em específico, a amostra do sinal 1 será realocado para o sinal 2, a amostra do sinal 2 será realocada para o sinal 3 e a amostra do sinal 3 será realocada para o sinal 1.

7. No caso da quarta iteração, já obtém o armazenado das posições realocadas de cada sinal correspondente as quatro primeiras amostras, como por exemplo:

$$K_{shuffled} = \begin{bmatrix} 2 & 3 & 1 \\ 3 & 2 & 1 \\ 2 & 1 & 3 \\ 1 & 2 & 3 \end{bmatrix}$$

8. Após completado a iteração para todas as amostras, a matriz $K_{shuffled}$ conterá todas as posições novas que as amostras irão assumir:

$$K_{shuffled} = \begin{bmatrix} 2 & 3 & 1 \\ 3 & 2 & 1 \\ 2 & 1 & 3 \\ 1 & 2 & 3 \\ & \vdots & \\ 3 & 2 & 1 \\ 2 & 1 & 3 \end{bmatrix}$$

9. Essa matriz é utilizada para o embaralhamento espectral das amostras como também será utilizada para o desembaralhamento espectral das amostras.