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

MARCELO PEREIRA NOGUEIRA

CRIPTOGRAFIA FÍSICA POR EMBARALHAMENTO ESPECTRAL APLICADA A SINAIS COM TAXAS DE TRANSMISSÃO DISTINTAS

SÃO JOÃO DA BOA VISTA
2022

MARCELO PEREIRA NOGUEIRA

CRIPTOGRAFIA FÍSICA POR EMBARALHAMENTO ESPECTRAL APLICADA A SINAIS COM TAXAS DE TRANSMISSÃO DISTINTAS

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

Orientador: Prof. Dr. Marcelo Luís Francisco Abbade

SÃO JOÃO DA BOA VISTA

2022

N778c

Nogueira, Marcelo Pereira

Criptografia física por embaralhamento espectral aplicada a sinais com taxas de transmissão distintas / Marcelo Pereira Nogueira. -- São João da Boa Vista, 2022

65 p.

Trabalho de conclusão de curso (Bacharelado - Engenharia de Telecomunicações) - Universidade Estadual Paulista (Unesp), Faculdade de Engenharia, São João da Boa Vista

Orientador: Marcelo Luís Francisco Abbade

Coorientador: Ivan Aritz Aldaya Garde

1. Criptografia. 2. Telecomunicações. 3. Segurança de sistemas. I. Título.

Sistema de geração automática de fichas catalográficas da Unesp. Biblioteca da Faculdade de Engenharia, São João da Boa Vista. Dados fornecidos pelo autor(a).

Essa ficha não pode ser modificada.

UNIVERSIDADE ESTADUAL PAULISTA "JÚLIO DE MESQUITA FILHO"
FACULDADE DE ENGENHARIA - CAMPUS DE SÃO JOÃO DA BOA VISTA
GRADUAÇÃO EM ENGENHARIA ELETRÔNICA E DE TELECOMUNICAÇÕES

TRABALHO DE CONCLUSÃO DE CURSO

CRIPTOGRAFIA FÍSICA POR EMBARALHAMENTO ESPECTRAL APLICADA A SINAIS COM TAXAS DE TRANSMISSÃO DISTINTAS

Aluno: Marcelo Pereira Nogueira
Orientador: Prof. Dr. Marcelo Luís Francisco Abbade

Banca Examinadora:

- Marcelo Luís Francisco Abbade (Orientador)
- Rafael Abrantes Penchel (Examinador)
- Welerson Santos Souza (Examinador)

A ata da defesa com as respectivas assinaturas dos membros encontra-se no prontuário do aluno (Expediente nº 096/2021)

São João da Boa Vista, 14 de fevereiro de 2022

DEDICATÓRIA

Dedico este trabalho à Deus, aos meus pais, à meu irmão, meus amigos, professores, funcionários e companheiros de pesquisa, que contribuiram com meu desenvolvimento pessoal, profissional e pelo carinho e auxílio que obtive durante todo o meu período acadêmico.

AGRADECIMENTOS

Agradeço a Deus primeiramente por todos os dias ajudar a me tornar uma pessoa melhor e estar presente em todos os momentos que passei durante a minha vida.

Ao meu orientador de pesquisa, Prof. Dr. Marcelo Luís Francisco Abbade, por ter me aceitado na equipe de pesquisa, pela paciência em me ensinar, por ter me inspirado em meu desenvolvimento pessoal e profissional. Fatores esses que me possibilitaram concluir trabalhos já realizados anteriormente e em especial pela realização deste Trabalho de Conclusão de Curso.

Ao meu coorientador Prof. Dr. Ivan Aritz Aldaya Garde, por ter tido paciência em me ensinar, mesmo nos momentos de dificuldades esteve ao meu lado junto com o Prof. Dr. Marcelo compartilhando o seu conhecimento e possíveis soluções para o desenvolvimento deste trabalho e de outros realizados pelo grupo de pesquisa.

Aos meu pais, Marcos Nogueira e Célia Pires Pereira Nogueira em conjunto com meu irmão Marcos Pereira Nogueira que me incentivaram a não desistir diante de todos os processos que passei durante o período da realização deste trabalho e de minha formação acadêmica.

Aos meus colegas de pesquisa e de turma, aos meus amigos que me incentivaram em todas as ocasiões, mesmo durante momentos conturbados, me ajudaram com um sorriso, carinho e amor.

“Não sou obrigado a vencer, mas tenho o dever de ser verdadeiro. Não sou obrigado a ter sucesso, mas tenho o dever de corresponder à luz que tenho”

(Abraham Lincoln)

RESUMO

A taxa de transmissão e o número de usuários de Internet têm aumentado consideravelmente em sistemas de comunicação. A preocupação da segurança e sigilo de dados gerados, transmitidos e armazenados tem se tornado uma característica de grande importância para o desenvolvimento e a evolução de tecnologias. A investigação, desenvolvimento e avaliação de novas melhorias para as técnicas de criptografias foram realizadas neste trabalho. As técnicas de criptografias investigadas foram codificação de fase espectral e embaralhamento espectral baseado em processamento digital de sinal (*spectral phase encoding and spectral shuffled in digital signal processing*, SPE-SS-DSP) com a implementação da chave dinâmica (*dynamic key*, DK) aplicado a sinais com taxas de transmissão distintas e sinalizações diferentes. As novas aplicações de melhora para as técnicas de criptografias foram avaliadas a partir de dois sinais criptografados e transmitidos por um canal com ruído aditivo, gaussiano e branco (*additive white Gaussian noise*, AWGN). O desenvolvimento dessas novas aplicações foi realizado por simulações computacionais. O Matlab® foi o *software* utilizado para implementar em algoritmo as técnicas de criptografias, a chave dinâmica, as novas aplicações, o canal ruidoso e a obtenção de resultados. A métrica de avaliação da qualidade do sinal e das novas aplicações para as técnicas de criptografias foi a penalização da razão sinal-ruído (*signal-to-noise ratio*, SNR) para um dado valor de razão de erro de bit (*bit error ratio*, BER). Os sinais criptografados possuíram valores de BER acima do limite da correção para frente de erro (*forward error correction*, FEC) e as novas aplicações não geraram penalidades aos sinais transmitidos e recuperados. Os sinais criptografados com chave dinâmica e aplicação de taxas de transmissão distintas e sinalizações diferentes comparando com os sinais sem criptografia e sem melhorias apresentaram resultados praticamente iguais com base nos valores de BER e SNR. As técnicas desenvolvidas, após avaliadas, mostraram uma boa eficiência e viabilidade de estudos e aplicações em redes ópticas e redes móveis.

Palavras-chave: segurança, criptografia, codificação de fase espectral, embaralhamento espectral, chave dinâmica, taxas de transmissões distintas, sinalizações diferentes.

ABSTRACT

The transmission ratio and the number of internet users have increased considerably in communication systems. The concern about security and secrecy of data generated, transmitted and stored has become a import characteristic for the development and technologies evolution. The investigation, development and evaluation of new improvements for encryption techniques were realized in this work. The techniques investigated were spectral phase encoding and spectral shuffled in digital signal processing (SPE-SS-DSP) with implemention of the dynamic key (DK) applied the signals with distinct transmission rates and with different signalings. The news improvements applications for encryption techniques were evaluated from two encrypted signals transmitted over channel with additive white Gaussian noise (AWGN). The development of these news applications were performed by computer simulations. The Matlab ® was software used to implement in algorithm the encryption techniques, dynamic key, news improvements applications, noise channel and the results obtained. The signal quality evaluation metric and new improvements applications for encryption techniques was the penalty of the signal-to-noise ratio (SNR) for given value of bit error ratio (BER). The encrypted signals showed BER values above forward error correction (FEC) threshold and the new applications didn't generate penalties for the transmitted and recovered signals. The signals encrypted with dynamic key, application of distinct transmission rates and with different signalings compared to signals without encryption and improvements showed pratically the same results based on BER and SNR values. The techniques developed, after being evaluated, showed good efficiency and feasibility of studies and applications in optical and mobile networks.

Keywords: security, cryptography, spectral phase encoding, spectral shuffled, digital signal processing, dynamic key, different rates, different signalings.

LISTA DE FIGURAS

LISTA DE SIGLAS E ABREVIATURAS

ADC	Conversor análogico digital
AES	Padrão de criptografia avançado
AWGN	Ruído Gaussiano aditivo branco
BL	Produto de taxa de bits-distância
BER	Razão de erro de bits
B2B	*Back-to-banck*
CAGR	Taxa de crescimento anual composta
DK	Chave dinâmica
DSP	Processamento de sinal digital
dB	Decibel
EON	Rede óptica elástica
FEC	Correção posterior de erro
FFT	Transformada rápida de Fourier
GBaud	Giga Baud
Gbps	Gigabits por segundo
ISI	Interferências intersímbolicas
IoE	Internet de todas as coisas
IFFT	Transformada rápida de Fourier inversa
ITU	União internacional das telecomunicações
kbps	kilobits por segundo
km	kilômetros
M2M	Máquina para Máquina
MCOESS	Codificação óptica por meio de embaralhamento espectral multi-canal
NMS	Sistema de gerenciamento de rede
OSI	Interconexão de sistemas abertos
OSNR	Razão de sinal-ruído óptico
PAM	Modulação por amplitude de pulso
PRBS	Sequência pseudoaleatória de bits
QAM	Modulação de amplitude em quadratura

QoS	Qualidade de serviço
QKD	Distribuição quântica de chaves
QPSK	Modulação por chaveamento de fase em quadratura
RCF	Filtro de cosseno levantado
SE-CF	Sinal embaralhado e criptografado em fase
SE-CF-TTD	Sinal embaralhado e criptografado em fase com taxas de transmissão distintas
SER	Razão de erro de símbolos
SCS	Sistemas caóticos sincronizados
SED-CDF	Sinal embaralhado/desembaralhado e codificado/decodificado em fase
SED-CDF-TTD	Sinal embaralhado/desembaralhado e codificado/decodificado em fase com taxa de transmissão distinta
SED-CDF-TTD-MD	Sinal embaralhado/desembaralhado, codificado/decodificado em fase com taxa de transmissão distinta e modulação distinta
SED-CDF-TTD-MD-CD	Sinal embaralhado/desembaralhado, codificado/decodificado em fase com taxa de transmissão distinta, modulação distinta e chave dinâmica
SNR	Razão de sinal ruído
SPE	Codificação espectral de fase
SPE-DSP	Codificação de fase espectral em DSP
SPE-SS-DSP	Embaralhamento espectral e codificação espectral baseado em DSP
SPDE	Códificação espectral de fase e atraso
SPDE-DSP	Codificação espectral de fase e atraso baseado em DSP
SPDE-SS-DSP	Embaralhamento espectral e codificação espectral de fase e de atraso baseado em DSP
SSC	Sinal sem criptografia
SS-DSP	Embaralhamento espectral baseado em DSP
TON	Redes ópticas transparentes
THz	Tera Hertz

LISTA DE SÍMBOLOS

$m_1[n]$	Primeiro sinal de entrada no domínio do tempo discretizado
$M_1[n]$	Primeiro sinal de entrada no domínio da frequência discretizada
$m_2[n]$	Segundo sinal de entrada no domínio do tempo discretizado
$M_2[n]$	Segundo sinal de entrada no domínio da frequência discretizada
$m[n]$	Sinal inicial complexo no domínio do tempo
$M[n]$	Sinal inicial complexo no domínio da frequência
B_S	Largura de banda limitada do sinal complexo no domínio da frequência pelo RCF
R_{sy}	Taxa de transmissão de símbolos
r	Fator de decaimento do RCF
P_s	Potência do sinal após filtro retângular no receptor
P_r	Potência de ruído após filtro retângular no receptor
exp	Exponencial (número natural)
f	Frequência
τ_i	Atraso da i-ésima amostra
φ_i	Fase da i-ésima amostra
n_{bits_falso}	Número de bits falsos
n_{bits_1}	Número de bits do primeiro sinal
n_{bits_2}	Número de bits do segundo sinal
$m_{1\_I}[n]$	Primeiro sinal no domínio do tempo discretizado correspondente a parte real
$m_{1\_Q}[n]$	Primeiro sinal no domínio do tempo discretizado correspondente a parte imaginária
$m_{1_{falso\_I}}[n]$	Primeiro sinal falso no domínio do tempo discretizado correspondente a parte real
$m_{1_{falso\_Q}}[n]$	Primeiro sinal falso no domínio do tempo discretizado correspondente a parte imaginária
$m_{1_{falso}}[n]$	Primeiro sinal falso no domínio do tempo discretizado
K_t	Chave temporária
K_i	Chave inicial

K_s	Chave semente
DK_1	Primeiro bloco da chave dinâmica
DK_2	Segundo bloco da chave dinâmica
DK_n	*n* bloco da chave dinâmica
DK_{n-1}	*n* do bloco da chave dinâmica anterior
m_1	Primeiro sinal no domínio do tempo
M_1	Primeiro sinal no domínio da frequência
m_2	Segundo sinal no domínio do tempo
M_2	Segundo sinal no domínio da frequência
c_1	Primeiro sinal criptografado no domínio do tempo
C_1	Primeiro sinal criptografado no domínio da frequência
c_2	Segundo sinal criptografado no domínio do tempo
C_2	Segundo sinal criptografado no domínio da frequência
r_1	Primeiro sinal criptografado e com ruído no domínio do tempo
R_1	Primeiro sinal criptografado e com ruído no domínio da frequência
r_2	Segundo sinal criptografado e com ruído no domínio do tempo
R_2	Segundo sinal criptografado e com ruído no domínio da frequência
d_1	Primeiro sinal descriptografado e recuperado no domínio do tempo
D_1	Primeiro sinal descriptografado e recuperado no domínio da frequência
d_2	Segundo sinal descriptografado e recuperado no domínio do tempo
D_2	Segundo sinal descriptografado e recuperado no domínio da frequêcia

SUMÁRIO

1. INTRODUÇÃO

A quantidade de taxa de transmissão de dados e o número de pessoas com acesso a Internet no mundo tem aumentado consideravelmente. A estimativa realizada pela CISCO em 2020 (CISCO, 2020) prevê que a taxa de crescimento anual composta (*compound annual growth rate*, CAGR) será de 10 % e até 2023 terá cerca de 5,3 bilhões de pessoas com acesso a Internet.

Segundo dados da União Internacional das Telecomunicações (*International Telecommunication Union*, ITU) em 2021 ocorreu o crescimento de usuários de Internet mais rápido do que o previsto pela CISCO devido a pandemia em 2020 e 2021 (ITU, 2021). A ITU menciona que aproximadamente 4,1 bilhões de pessoas (54 % da população mundial) estavam utilizando a Internet em 2019 e atualmente em 2021 tem atingido 4,9 bilhões de usuários de Internet (63 % da população mundial). Durante a pandemia (2019 – 2021) houve um crescimento de 17 %, sendo estimado cerca de 782 milhões de pessoas que se tornaram usuários de Internet (ITU, 2021). Na Figura 1 é apresentada a estimativa realizada pela ITU e disponibilizada em (ITU, 2021) e (ITU DEVELOPMENT SECTOR, 2021) para acesso ao público sobre o crescimento anual de usuários de Internet no período de 2005 a 2021.

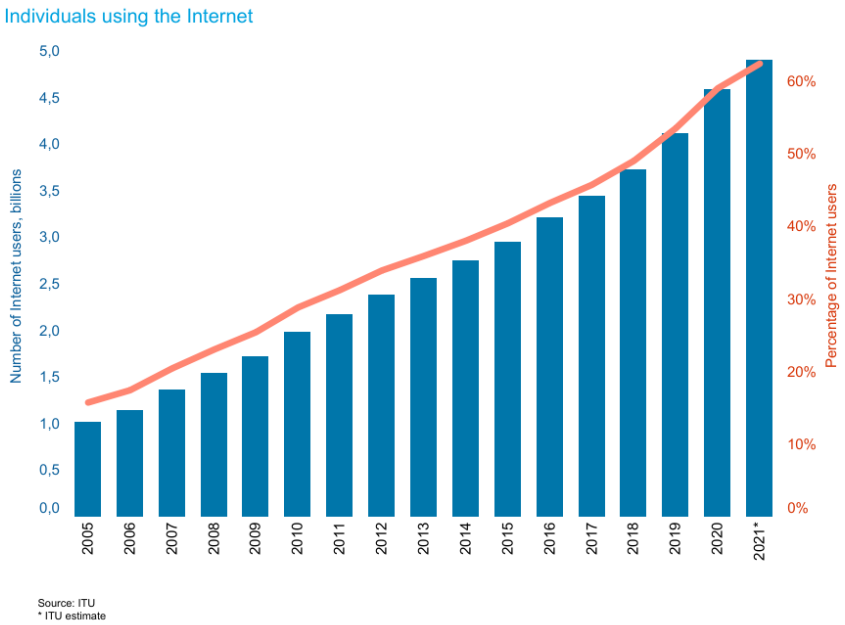

Figura 1 - Crescimento do número de usuários de Internet ao longos dos anos (2005 – 2021).[1]

[1] Fonte*: Internet Telecommunications Union*, 2021

O número de pessoas sem acesso à Internet é de 2,9 bilhões, sendo que 96 % vivem em países em desenvolvimento e cerca de 390 milhões de pessoas não têm cobertura de um sinal de banda larga móvel (ITU DEVELOPMENT SECTOR, 2021). Nós próximos anos, de acordo com esses dados, a Internet chegará a mais pessoas e o número de usuários de Internet tenderá a aumentar ainda mais.

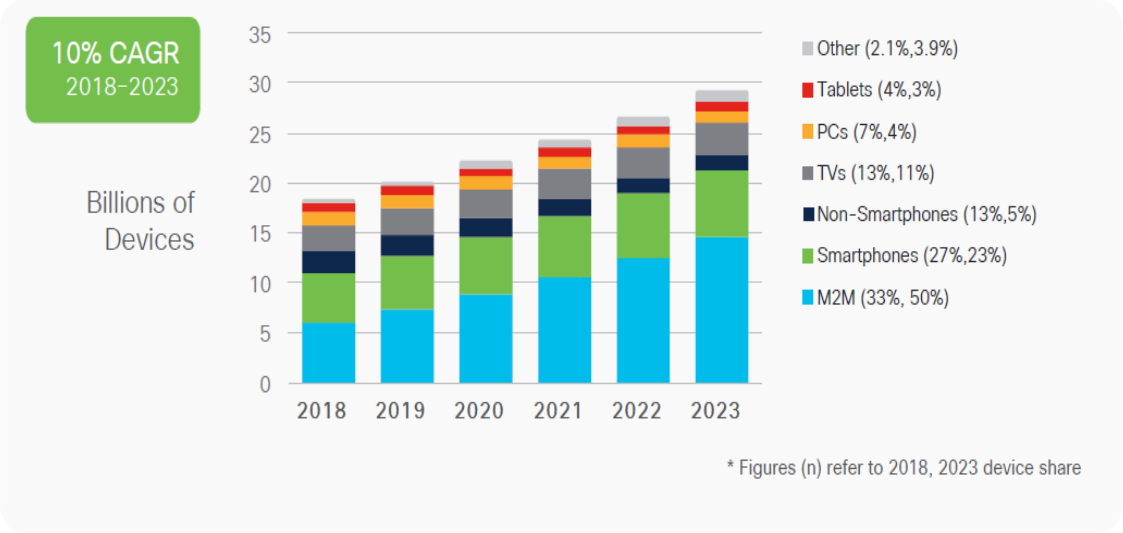

Figura 2 - Estimativa do crescimento da utilização de aparelhos eletrônicos ao longo dos anos (2018 – 2023) com uma CAGR de 10 %.[2]

O aumento da quantidade de usuários de Internet em conjunto com o aumento da taxa de transmissão, que é possibilitada pela tecnologia de redes móveis 5G (FARIAS, 2019) e pelo desenvolvimento da fibra óptica, estão provocando não apenas uma interconexão entre celulares e computadores, mas também de outros dispositivos, como exemplo, geladeiras, TVs, lampâdas, relógios, ar condicionados e óculos. Na Figura 2 é mostrada o gráfico disponibilizado pela CISCO e são estimados as porcentagens de utilização de diversos aparelhos eletrônicos entre o ano de 2018 e 2023 (CISCO, 2020). As interconexões de diversos dispositos em massa gerará um ecossistema interconectado (CISCO, 2014), chamado de Internet de todas as coisas (*Internet of everything*, IoE). A porcentagem de comunicação máquina para máquina (*machine to machine*, M2M) possui um crescimento maior do que a de *smartphones* como mostrado na Figura 2, o que tenderá a ser ainda maior nós próximos anos devido à grande interconexão entre os mais diversos aparelhos.

[2] Fonte: *Cisco Annual Internet Report*, 2018–2023

Diante desse cenário, é discutido um tópico de grande importância sobre o quão seguro é a transmissão de dados e o quanto a implementação de técnicas de seguranças afeta na qualidade de serviço (*quality of service*, QoS).

1.1. Importância das comunicações de rede móveis e das comunicações ópticas

Os próximos paragráfos descrevem sucintamente a evolução das comunicações móveis e das comunicações ópticas. Esta Seção mencionará as altas taxas de transmissão alcançadas e será comentado sobre as tecnologias estudadas atualmente para suprir as demandas de mercado, como o tráfego de dados, as altas taxas de transmissão e o alto número de usuários de Internet.

O setor de rede móvel nos últimos anos tem crescido significativamente até os dias atuais. A Figura 3 ilustra as evoluções das tecnologias de sistema de comunicações móveis. Exemplo da tecnologia 1G, que possuia serviço apenas de voz (totalmente analógica), até a tecnologia 5G, que possui serviços de nuvem, endereçamento IP, banda larga móvel com altas taxas de transmissão (FARIAS, 2019). A tecnologia 2G em 1991 possuia uma taxa de 384 kbps e atualmente em 2021 a tecnologia 5G possui uma taxa de transmissão que chega-se a 20 Gbps para *downlinks* (FARIAS, 2019).

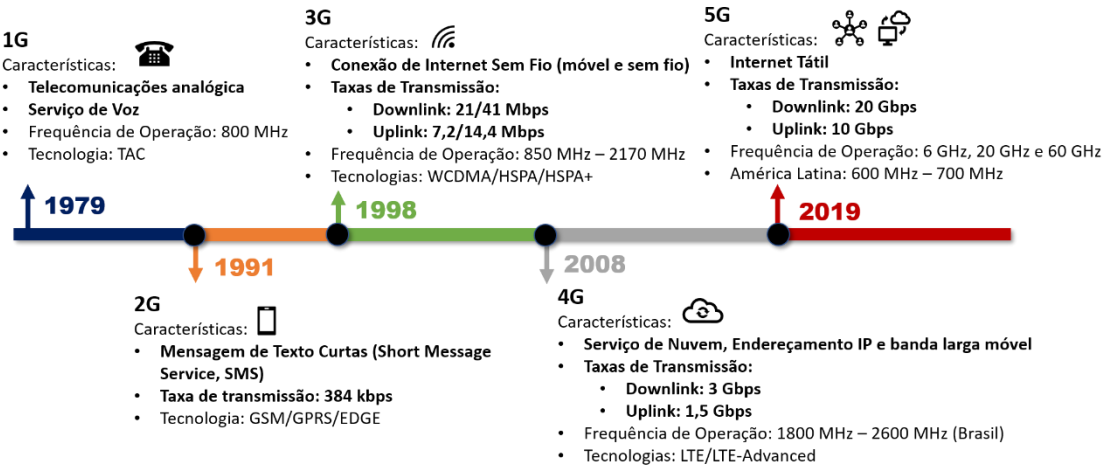

Figura 3 - Evolução das tecnologias 1G até a 5G e as principais características de cada tecnologia ao longo do tempo. Fonte: Autoria própria.

O setor de comunicação óptica também é exemplo da extrema importância para transmissão de informações. Em (AGRAWAL, 2014) menciona-se a emergência da tecnologia de comunicação óptica a partir da década de 1970. Desde 1975 até os anos 2000 apresentou uma evolução com um aumento exponencial no produto taxa de bit-distâcia (*bit rate-length product*, BL), unidade em $bits/s - km$. Esse aumento foi de 10^6

$bits/s - km$ até próximo de 10^{15} $bits/s - km$, graças as tecnologias desenvolvidas desde o telégrafo, telefone, cabos coaxiais, micro-ondas, ondas luminosas e amplificadores ópticos (AGRAWAL, 2014). Outro fator de relevância é o aumento linear da capacidade-distância ($Gb/s \cdot km$) considerando o progresso de sistemas de comunicação por fibra óptica realizado em 25 anos. Entre 1975 e 2000 temos um aumento desde da Primeira Geração até a Quarta Geração de 10^1 até aproximadamente 10^7 $Gb/s \cdot km$ (AGRAWAL, 2014).

As comunicações ópticas adotam tecnologias de modulação avançada, correção posterior de erro (*forward error correction*, FEC) e sistemas de detecção coerente. Segundo (SOMA, 2018), em setembro de 2017 foi possível transmitir 10,16 Pb/s utilizando fibras multimodos. Os recordes de capacidade e de taxa de transmissão de dados para cabos submarinos são de 30 Tb/s e 700 Gb/s, respectivamente. O aumento da eficiência espectral de cada sinal, selecionando uma distribuição de símbolos para maximizar os dados transportados foi requerido para que a capacidade de 30 Tb/s fosse alcançada (WILKINSON, 2021).

Há diferentes tipos de modulações que podem ser aplicadas ao sinal dependendo das características e considerações do projeto da rede que será implementada. Como exemplo de modulações utilizadas em sistemas de comunicações, temos a modulação por chaveamento de fase em quadratura (*quadrature phase shift keying*, QPSK) e a 16 modulação de amplitude em quadratura (*quatrature amplitude modulation*, 16-QAM). Essas modulações são descritas com mais detalhes em (LATHI; DING, 2012).

Segundo (GERSTEL, 2012) a modulação *on-off* de sinais, que era adequada para taxas de bits de até 10 Gb/s, evoluiu para esquemas de modulação mais sofisticados para taxas de 100 Gb/s. Nos sistemas de comunicações ópticas é conveniente acomodar elevada banda para a utilização mais eficiente do espectro óptico com uma grade mais flexível (GERSTEL, 2012). A rede mais flexível origina um novo paradigma de rede óptica elástica (*elastic optical network*, EON). A EON terá que atender alguns requisitos para tornar uma rede flexível, sendo esses requisitos: suportar uma demanda por taxas de transmissão maiores que 400 Gb/s por canal, atender a necessidade de largura de bandas distintas e ter um espaçamento de canais mais estreito (ZHANG *et al.*, 2013).

1.2. Segurança e criptografia em comunicações ópticas e em redes móveis

As comunicações ópticas e móveis possuem atualmente altas taxas de dados transmitidos e, como mencionado, a tendência será aumentar ainda mais a quantidade de informações transmitidas e o número de pessoas que serão usuários de Internet. As redes de comunicação atuais e futuras se tornam sensíveis às falhas de comunicação causadas por falhas de componentes ou ataques deliberados. Uma rede segura deve fornecer segurança física de comunicação. A discussão pautada e de extrema importância é sobre a garantia de um certo nível de QoS em relação à segurança, a integridade de dados e a privacidade de comunicação.

A revista The Times e The Register publicaram notícias de vunerabilidade e preocupação com a segurança na transmissão de dados por fibra óptica. A revista The Times publicou em fevereiro de 2020 que a Rússia enviou agentes de inteligência à Irlanda para mapear a localização precisa de cabos transatlânticos (MOONEY, 2020). A Irlanda é um ponto de desembarque dos cabos submarinos que transportam o tráfego da Internet entre a América e a Europa (TELEGEOGRAFY, 2021), destacando-se como região de importância geopolítica. As demais agências de inteligência temem que a Rússia planeje realizar novas operações de espionagem cibernética grampeando os cabos submarinos (MOONEY, 2020). Outro fato semelhante foi publicado em 2014 pelo jornal The Register sobre uma base de espiões britânicos localizada em Seeb na costa norte de Omã (CAMPBELL, 2014). A costa de Omã é uma posição estratégica que permite explorar os cabos submarinos que passam pelo estreito de Ormuz no Golfo Pérsico (TELEGEOGRAFY, 2021). Grande parte dos cabos submarinos utilizam fibras ópticas, como exemplo, a empresa Apollo Submarine Cable System é responsável pelos cabos transatlânticos entre os Estados Unidos e a Europa. Apollo é um sistema de cabos submarinos de comunicação óptica de 13000 km de comprimento que cruza o oceano Atlântico. O sistema consiste em dois cabos de fibra óptica transatlânticos mais avançados: Apollo North, que conecta o Reino Unido e os Estados Unidos e o Apollo South, que conecta a França e os Estados Unidos (CAMPBELL, 2014).

As informações enviadas pelo interior da fibra óptica conferem maior segurança do que a rede móvel, pois transmitem os sinais por um canal guiado, enquanto que a rede móvel por um canal não guiado. A rede óptica, mesmo assim, ainda esta vunerável a ataques que utilizam dispositivos capazes de adquirir informações que estão passando pelas fibras ópticas. Os dispositivos mais comuns para realizar as extrações de informações das fibras ópticas são grampos ópticos passivos (*passive fiber clip-on*

coupler) e o ociloscópio de inspeção em fibra (*fiber inspection scope*) disponíveis em (ETERNAL) e (EXFO). Alguém que tenha acesso a esses dispositivos pode coletar informações que estão sendo transmitidas pelas redes ópticas por meio do desvio dos feixes de luzes das fibras ópticas (BOBADILHA, 2018).

Em (FURDEK; SKORIN-KAPOV, 2012) são mencionadas as etapas para agir contra ataques e falhas utilizadas pelo sistema de gerenciamento de rede (*network management system*, NMS). O NMS proposto deve realizar as seguintes etapas quando há um ataque ou falha:

1. Detectar o ataque: Descobrir se há deterioração da qualidade do sinal, uma intrusão na fibra, perda de serviço ou qualquer outra consequência direta de um ataque;
2. Localização do ataque: identificar o local e a fonte do ataque;
3. Reagir ao ataque: acionando mecanismos de reação. O ponto de acesso do atacante deve ser isolado e os efeitos nocivos devem ser neutralizados. As conexões afetadas devem ser restauradas e as comunicações devem ser retomadas.

As três etapas de reação contra ataques e falhas demandam muito processamento e tempo. Inspecionar toda a extensão da fibra óptica, por exemplo, é fisicamente e economicamente inviável. Há outras formas da rede se manter segura e de forma preventiva, como as técnicas de criptografias na camada física com base em DSP (ABBADE *et al.*, 2020). As técnicas de criptografias são implementadas nas diversas camadas do modelo de referência para interconexão de sistemas abertos (*open system for interconnections*, OSI), descritas em (IOS, 1984). O interesse em desenvolver técnicas de criptografia em camada física, como mencionadas em (ABBADE *et al.*, 2020) é que quanto maior a quantidade de camadas incorporadas do modelo OSI, mais seguro estão as informações (KITAYAMA, 2011). A camada física é a última antes do sinal ser transmitido e trafegado, logo, contém todas as criptografias das camadas anteriores.

As abordagens de segurança computacional para comunicação sem fio, por exemplo em (RIVEST; SHAMIR; ADLEMAN, 1978) e (DIFFIE; HELLMAN, 1976) funcionaram bem na prática, porém ataques bem sucedidos foram relatados nesses mecanismos de seguranças ao longo dos anos, como exemplo em (SCHNEIER; KELSEY, 1976) e (BIRYUKOV; SHAMIR; WAGNER, 2001). A criptografia na camada

física tem motivado o interesse em estudos e aplicações dos princípios de segurança da teória da informação e do processamento de sinais para proteger os sistemas da camada física. Em (YENER; ULUKUS, 2015) é relatada a possibilidade de segurança na camada física a partir da teoria de informação e é comentado sobre estudos de sigilo em cenários de comunicação sem fio com múltiplos transmissores, mencionando as diversas formas de um intruso obter as informações e dados ilegamente dos dispositivos sem fio.

1.3. Criptografia na camada física

As criptografias na camada física que se destacam são a criptografia caótica, quântica, codificação espectral de fase e atraso, codificação espectral de fase e atraso com base em DPS, criptografia óptica mediante fatiamento e embaralhamento espectrais e embaralhamento espectral aplicado em redes ópticas com base em DSP. A chave dinâmica é uma estratégia para cálculo de uma nova chave criptográfica para cada bloco, que é encriptado. A seguir serão comentados os trabalhos desenvolvidos sobre cada uma dessas criptografias e sobre o algoritmo de chave dinâmica realizados na camada física.

A criptografia caótica tem sido uma proposta com potêncial de fornecer um alto nível de robustez e privacidade nas transmissões de dados sem especificar o meio de comunicação como descrito em (CUOMO; OPPENHEIM; STROGATZ, 1993) e (COLET; ROY, 1994). Duas abordagens possíveis para comunicações seguras são demonstradas com o circuito de Lorenz implementado no transmissor e receptor (CUOMO; OPPENHEIM; STROGATZ, 1993). As duas abordagens usam o conceito de sistemas caóticos sincronizados (*synchronized chaotic systems*, SCS), que dependem da robustez da sincronização diante das perturbações sofridas pelo sinal. Em (COLET; ROY, 1994) é proposto um esquema para codificar dados digitais dentro de uma portadora caótica. A decodificação é realizada em tempo real com um sistema de laser caótico sincronizado. Os sinais transmitidos ao longo dos enlaces ópticos e redes sem fio sofrem impacto do próprio canal de transmissão e dificulta a sincronização entre o transmissor e o receptor (ABBADE *et al.*, 2013). Porém mesmo diante dessas dificuldades de sincronização em (FAN *et al.*, 1998) foi realizado uma demonstração da comunicação de longa distância e com alta taxa com base na sincronização caótica em um canal de fibra óptico comercial. A decodificação foi realizada a partir de um segundo laser, que ao sincronizar com a portadora caótica gerada no transmissor permite a separação da portadora e da mensagem. A distância do enlace de fibra óptica responsável pela transmissão foi de 120 km.

A criptografia quântica vem sendo desenvolvida para proporcionar maior segurança nos meios de comunicações, porém possui como desvantagem baixas taxas de transmissão (KARTALOPOULOS, 2007). Segundo (IDQ REDEFINING SECURITY, 2020) a criptografia quântica é uma tecnologia para proteger a distribuição de chaves criptográficas, chamada de distribuição quântica de chaves (*quantum key distribuition*, QKD). A técnica é baseada em enviar partículas quânticas por meio de um canal. Como exemplo dessa técnica, os sinais a serem transmitidos são codificados e decodificados aleatoriamente utilizando um único pulso de fóton. Esse pulso de fóton ocupa estado de polarização aleatório e pode ser formado pelo emissor e pelo receptor a qualquer momento por meio de um canal quântico (SUCHAT; PAIBOON; YUPAPIN, 2002). No princípio da física quântica, a observação de um estado quântico causa perturbações e os vários protocolos QKD aproveitam desse princípio para garantir que qualquer tentativa de um intruso em observar os fótons transmitidos perturbará a transmissão. A perturbação realizada pelo intruso, caso houver, causará erros de transmissão que podem ser detectados pelos usuários legais da rede (IDQ REDEFINING SECURITY, 2020). As desvantagens descritas em (KARTALOPOULOS, 2007) são o limite de 97 km e o alto custo de implementação (LYDIA; SMAIL; MOHAMED, 2017).

A codificação espectral de fase e atraso (*spectral phase and delay encoding*, SPDE) é um aprimoramento da codificação espectral de fase (*spectral phase encoding*, SPE) com base em (CORNEJO; TOCNAYE, 2008) e é uma técnica de criptografia que pode ser aplicada em redes ópticas transparentes (*transparent optical networks*, TON), como estudado em (ABBADE *et al.*, 2014). A técnica realiza a divisão de *n* fatias espectrais de um sinal e, posteriormente, na fase de cada fatia é inserido uma diferença de fase e de atraso. O resultado das simulações em (ABBADE *et al.*, 2015) mostram que é possível a propagação dos sinais criptografados por mais de 400 km. As avaliações dos sinais foram feitas para sinais modulados em QPSK e 16-QAM com taxas de transmissões de 40 Gbps e 200 Gbps.

A versão em DSP da técnica de codificação espectral de fase e atraso, chamada de codificação em fase e atraso baseada em DSP *(spetral phase and delay encoding digital signal processing*, SPDE-DSP), possui a ideia semelhante da SPDE porém com a implementação da criptografia do sinal desenvolvida em algoritmo. A técnica em DSP foi simulada para uma TON. A chave criptográfica gerada possibilita recuperar o sinal

original. O trabalho foi desenvolvido para integrar mais robustez as técnicas de criptografias desenvolvidas pelo grupo de pesquisa (SANTOS, 2020).

A técnica de criptografia mediante fatiamento e embaralhamento espectral em um meio totalmente óptico foi investigada por meio de simulações computacionais e os sinais criptografados foram transmitidos por uma rede TON (BOBADILHA, 2018). A técnica é denominada codificação óptica por meio de embaralhamento espectral multi-canal (*multi-channel optical Encoding with spectral shuffling*, MCOESS). A técnica MCOESS é baseada na divisão espectral em *n* fatias de dois sinais e, posteriormente, ocorre o embaralhamento de cada fatia entre esses sinais. O embaralhamento é definido como a troca ou não da *i*-ésima fatia do primeiro sinal pela *i*-ésima fatia do segundo sinal baseado em uma chave criptográfica, que contém valores correspondentes a realização da troca ou não de fatias. Os resultados do trabalho mostraram um alcance de enlace de fibra óptica de 560 km para um canal óptico com ruído Gaussiano aditivo branco (*additive white Gaussian noise*, AWGN) com 0, 128, 256 e 330 fatias embaralhadas. Os resultados obtidos foram a partir da análise feita entre a razão de erro de bits (*bits error ratio*, BER) em relação a razão de sinal-ruído óptico (*optical signal-to-noise ratio*, OSNR). A penalidade da OSNR no limite da FEC do sinal transmitido por um canal AWGN em comparação com o sistema *back-to-back* (B2B) foi de apenas 0,5 dB.

O embaralhamento espectral baseado em DSP (*spectral shuffling digital processing*, SS-DSP), aplicado em redes ópticas foi desenvolvido como um projeto de iniciação científica em (NOGUEIRA, 2019) e também publicado em (ABBADE; NOGUEIRA *et al.*, 2020). A técnica de criptografia desse trabalho foi desenvolvida em DSP e em banda base e, posteriormente, os sinais criptografados foram modulados e transmitidos pela TON utilizando um ambiente computacional de simulação. A técnica é baseada na divisão espectral em *n* fatias dos sinais gerados no transmissor. Posteriormente, essas fatias são embaralhadas entre esses sinais. O embaralhamento é definido como a troca ou não da *i-ésima* fatia do *i*-ésimo sinal pela *i*-ésima fatia do *i*-ésimo sinal. As posições das fatias espectrais que são trocadas e para qual sinal serão armazenadas estão contidas em uma chave criptográfica. No processo de desembaralhamento, após a transmissão do sinal criptografado, é utilizado essa chave para o desembaralhamento e as fatias espectrais são retornadas aos seus respectivos sinais e nas posições originais. Os resultados das simulações em (NOGUEIRA, 2019) referente à transmissão de dois e quatro sinais criptografados em SS-DSP em uma mesma rota

mostram um alcance entre 720 km e 800 km de comprimento de fibra óptica para uma taxa de transmissão de 112 Gbps com uma modulação 16-QAM. Em (ABBADE; NOGUEIRA *et al.*, 2020) também consta resultados de dois sinais criptografados em SS-DSP com uma taxa de transmissão de 112 Gbps e modulação de 16-QAM. Um desses sinais foi transmitido por uma rota fixa de 480 km e o outro foi transmitido por uma rota variável. O sinal transmitido pela rota variável alcançou entre 720 km e 800 km o limite da FEC para um valor de BER igual a $2 \cdot 10^{-3}$ e para uma largura de banda de 14,28 GHz. O sinal transmitido com rota fixa em 480 km alcançou o limite da FEC praticamente no mesmo ponto em que o sinal transmitido com rota variável. A transmissão dos sinais por rotas diferentes aumenta a dificuldade do intruso em obter as informações contidas nos sinais, uma vez que, como as fatias espectrais estão embaralhadas entre os sinais, é necessário para realizar o desembaralhamento possuir todos os sinais, o que é despendioso, demanda tempo e um processamento de dados maior em comparação com o caso dos sinais transmitidos por apenas uma única rota.

O trabalho em (NOGUEIRA, 2019) apresenta os resultados da técnica SS-DSP em conjunto com a técnica SPDE-DSP para aumentar a robustez da segurança das informações transmitidas pelo canal óptico. A técnica chamada de embaralhamento espectral e codificação espectral de fase e de atraso baseado em DSP (*spectral phase and delay encoding – spectral shuffled digital signal processing*, SPDE-SS-DSP). Os resultados mostram que as duas técnicas de criptografias aumentaram a segurança dos sinais transmitidos, enquanto que o alcance atingido no limite da FEC após a transmissão dos sinais por uma rede óptica foi praticamente o mesmo em comparação da técnica SS-DSP (entre 720 km e 800 km) como mencionado em (ABBADE; NOGUEIRA *et al.*, 2020).

A proposta de chave dinâmica (*dynamic key*, DK) foi desenvolvida em (NGO, 2010) e é mencionada como um meio para reduzir os riscos de ataques deliberados. As chaves dinâmicas utilizam chaves criptográficas simétricas e a teoria pode ser aplicada para melhorar a segurança e o desempenho de sistemas de criptografias. A DK é aplicada para garantir a segurança da informação transmitida a partir das propriedades estabelecidas por Shannon.

As propriedades estabelecidas por Shannon em (SHANNON, 1949) são a difusão e a confusão. A difusão é uma propriedade em que se alterar um bit da mensagem de

entrada, os dados da mensagem criptografada variam em aproximadamente 50 % dos bits. O que comprova a não existência de nenhuma relação entre a mensagem de entrada e a mensagem criptografada, dificultando ao intruso descobrir alguma informação da mensagem original. A confusão é uma propriedade em que se um bit da chave criptográfica for alterado, majoritariamento os bits da mensagem criptografada também devem ser alterados. A confusão é garantida se, em média, 50 % dos bits da mensagem criptografada forem alterados.

A criptografia codificação de fase espectral e embaralhamento espectral baseado em DSP (*spectral phase encoding – spectral shuffled digital signal processing*, SPE-SS-DSP) com aplicações de DK, dificulta ainda mais a ação de qualquer intruso. Recentemente em (SOUZA *et al.*, 2020) e (ABBADE; SOUZA *et al*., 2020) as técnicas de criptografias de sinais SPE-SS-DSP incorporaram também a técnica de DK. Os sinais são gerados e criptografados em blocos e posteriormente são concatenados os blocos e transmitidos os sinais por um canal óptico. No processo de decodificação é realizado a descriptografia em blocos. Em (SOUZA *et al.*, 2020) e (ABBADE; SOUZA *et al*., 2020) também foram realizadas simulações para garantir as propriedades de Shannon.

1.4. Contribuições do trabalho

Durante o desenvolvimento do trabalho contribuiu com a incorporação das técnicas SPDE-SS-DSP com chave dinâmica publicado em (SOUZA *et al.*, 2020). A partir desse trabalho começou o estudo de incoporação de demais melhorias que serão avaliadas neste trabalho.

Neste trabalho avalia-se a técnica de transmissão de dois sinais criptografados em SPE-SS-DSP com DK aplicando as melhorias de taxas de transmissão distintas e de sinalizações diferentes em um canal AWGN. As principais contribuições desses resultados são:

- A avaliação e comparação em relação a qualidade dos sinais entre as técnicas de criptografia SPDE-SS-DSP com DK e as técnicas SPDE-SS-DSP com chave dinâmica aplicadas a sinais com taxas de transmissão distintas;
- Avaliação e comparação em relação a qualidade dos sinais entre as técnicas SPDE-SS-DSP com DK aplicadas a sinais com taxas de transmissão distintas e as técnicas SPDE-SS-DSP com DK aplicadas a

sinais com taxas de transmissão distintas incluíndo sinalizações diferentes (QPSK e 16-QAM).

O autor, além da pesquisa acerca das melhorias propostas neste trabalho, também participou das atividades do grupo em relação ao desenvolvimento de novas técnicas de criptografias. Os trabalhos em que o autor possui participação foram: contribuição de alguns resultados para a versão totalmente óptica da técnica para embaralhar e desembaralhar sinais, sendo apresentado como trabalho convidado para o 21st *International Conference on Transparent Optical Networks* (BRAGAGNOLLE *et al.*, 2019); contribuição e desenvolvimento do código da criptografia de embaralhamento e desembaralhamento em processamento digital de sinal aplicado em TONs, obteve a maioria dos resultados apresentados em (ABBADE; NOGUEIRA *et al.*, 2020) e o trabalho foi publicado na *IEEE Photonics Technology Letters*; contribuição de alguns resultados e auxílio na junção das técnicas SPDE-SS-DSP com DK no *software* KryptoSJ sendo apresentado como trabalho convidado para a *International Conference on Transparent Optical Networks* (SOUZA *et al.*, 2020) e para a *Advanced Photonics Congress* (ABBADE; SOUZA *et al*., 2020).

As duas melhorias desenvolvidas nesse trabalho são de interesse em particular de comunicação óptica em redes elásticas (ZHANG *et al.*, 2013). A implementação práticas dessas melhorias pode ser feita em trabalhos futuros, podendo possuir aplicações em empresas, intituições governamentais, bancos, operadoras e qualquer meio que exija um alto nível de confidencialidade. As melhorias desenvolvidas são estudadas e implementadas para promover maior segurança na transmissão de informações pelo canal.

1.5. Organização do trabalho

O primeiro Capítulo abordou a motivação e a importância de segurança em comunicações móveis e ópticas, o desenvolvimento de técnicas de segurança em camada física e a contribuição deste trabalho para com as demais técnicas de criptografias já existentes com objetivo de manter o sigilo de dados. Os demais capítulos estão organizados na seguinte ordem. No Capítulo 2 a organização do código é descrita e são explicadas as técnicas de criptografias já existentes e incorporadas ao código em conjunto com as melhorias desenvolvidas neste trabalho. As novas melhorias são a transmissão de sinais com taxas distintas e sinalizações diferentes. No capítulo 3 são citados os

parâmetros utilizados durante as simulações e discutidos os resultados obtidos considerando um canal sem ruído e com ruído. O Capítulo 4 conclui o trabalho com considerações finais pertinentes em relação ao trabalho desenvolvido.

2. ORGANIZAÇÃO E DESCRIÇÃO DO CÓDIGO

A organização do código e as técnicas de criptografias são descritas neste Capítulo, que está dividido em duas Seções. A Seção 2.1 descreverá os módulos e as funções correspondentes à geração, transmissão e recepção de sinais. A Seção 2.2 descreverá as técnicas de criptografias aplicadas aos sinais, o algoritmo de DK e as novas melhorias desenvolvidas neste trabalho.

Convencionou-se 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 representará o sinal será "m" ou "M" acompanhada de um número natural e inteiro, que representará se o sinal é o primeiro ou o segundo. Exemplo: $m_1[n]$ é o primeiro sinal no domínio do tempo; $M_1[n]$ é o primeiro sinal no domínio da frequência; $m_2[n]$ é o segundo sinal no domínio do tempo e $M_2[n]$ é o segundo sinal no domínio da frequência. Os sinais $M_1[n]$ e $M_2[n]$, respectivamente, são a transformada rápida de Fourier (*fast Fourier transform*, FFT) dos sinais $m_1[n]$ e $m_2[n]$ (LATHI; DING, 2012).

O diagrama da Figura 4 representa a organização esquemática do código incluindo os módulos de criptografia que foram aplicados neste trabalho. As técnicas descritas nas Subseções a seguir foram incorporadas em conjunto no *software* KryptosSJ. O código foi e é desenvolvido por um grupo de pesquisa e apresenta variações de sua versão, porém com objetivo de incorporar todas as técnicas em apenas um código é mantido atualizado e chamado de KryptoSJ em sua versão final. No código atual, desenvolvido neste trabalho, estão incoporadas as técnicas de criptografias de fase e atraso, embaralhamento e desembaralhamento, transmissão de sinais com taxas distintas, modulações diferentes e chave dinâmica. Todo o desenvolvimento do código foi realizado no *software* Matlab®.

O código aplica as técnicas de criptografias em sinais multi-níveis com sinalização por amplitude de pulso (*pulse amplitude modulation*, PAM), sendo 2-PAM e 4-PAM complexos, que quando modulados geram sinais com modulação QPSK e 16-QAM respectivamente. O sinal composto por uma componente real 2-PAM e por uma componente imaginária 2-PAM será chamado de equivalente QPSK em banda base. O sinal composto por componentes real e imaginária 4-PAM será denominado de equivalente 16-QAM em banda base.

O diagrama representativo da Figura 4 possui três módulos, sendo o "Transmissor", "Canal" e "Receptor". Cada módulo é dividido em submódulos sendo

“Geração de Chaves Criptográficas”, “Geração e Criptografia de Sinais em Blocos”, “ADC”, “Descriptografia de Sinais em Blocos”, “FFT”, “RCF”, “IFFT”, “Demapeador”, “Parâmetros” e “Parâmetros 2”. No interior dos submódulos estão as funções que serão descritas durante a explicação do código a seguir. Os módulos que possuem o mesmo nome das funções são “FFT”, “RCF” e “IFFT”. Esses submódulos e funções contém as mesmas finalidades e aplicações durante o código, por isso são designados com o mesmo nome.

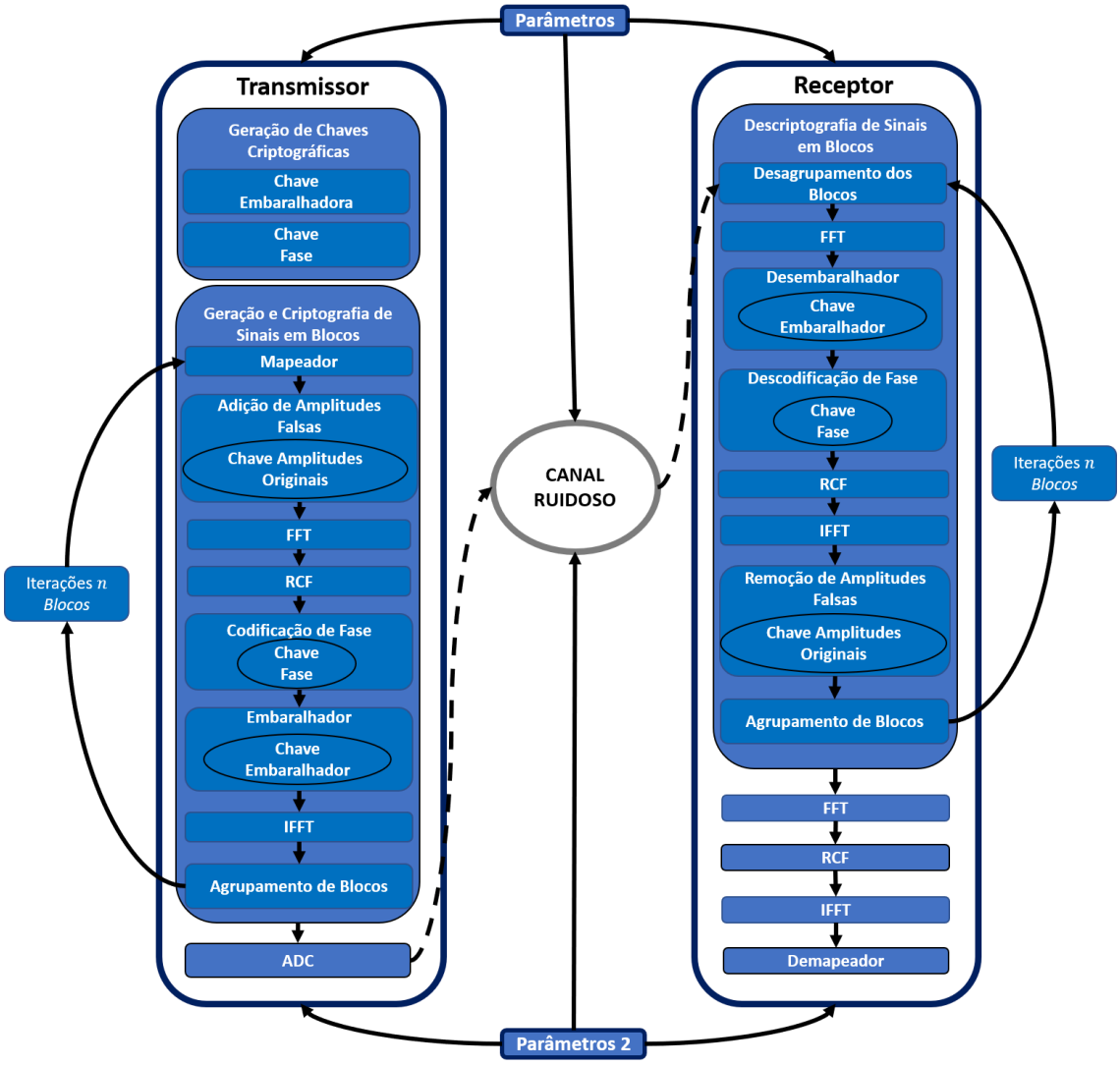

Figura 4 - Diagrama representativo sobre a organização esquemática do código. Fonte: Autoria própria.

Os submódulos “Parâmetros” e “Parâmetros 2” destacam-se, pois possuem valores de parâmetros atribuídos em variáveis que são necessárias ao longo de todo o código. Esses submódulos são carregados nos módulos “Transmissor”, “Canal” e “Receptor”. Os exemplos de parâmetros são: o número de amostras; tipo de modulação;

taxa de transmissão; frequência de amostragem; tempo de amostragem; banda do sinal; banda codificada do sinal e as opções de aplicar ou não as técnicas de criptografia desenvolvidas.

2.1. Geração, transmissão e recepção de sinais

A Seção 2.1 é dividida de acordo com os módulos da Figura 4. Na Subseção 2.1.1 será descrita acerca dos submódulos e funções correspondentes ao módulo "Transmissor". Na Subseção 2.1.2 será descrita em relação ao módulo "Canal Ruidoso" e a subseção 2.1.3 será descrita em relação ao módulo "Receptor".

2.1.1. Transmissor

Os sinais são gerados na função "Mapeador" a partir de uma sequência pseudoaleatória de bits (*pseudo random bit sequence*, PRBS), que são mapeados em símbolos associados aos eixos I e Q em acordo com o tipo de sinalização utilizada. Por exemplo, caso utilizar a modulação QPSK terá 2 bits por símbolo e se utilizar a modulação 16-QAM terá 4 bits por símbolo. A seguir, são atribuídas amplitudes ao sinal de acordo com o tipo de sinalização utilizada. Cada valor de amplitude na palavra é dobrado e inserido valores nulos nas posições pares. A amostragem, dessa forma, será feita nas posições ímpares da palavra. Após essa atribuição de valores de amplitudes é associado o eixo I com o eixo Q e gerado o sinal inicial complexo $m[n]$. Exemplo de uma parte do sinal inicial com modulação em 16-QAM:

$m[n]$ = [-3-3i 0+0i 3+1i 0+0i -3+1i 0+0i 3+1i 0+0i -1-3i 0+0i -3 - 3i 0+0i 1-1i]

A segunda função abordada é a "FFT", que é responsável por passar o sinal do domínio do tempo para o domínio da frequência. O submódulo chamado de "RCF" é responsável por passar o sinal inicial por um filtro de Nyquist com perfil de cosseno levantado (*raised cossine filter*, RCF) para prover proteção contra interferências intersimbólicas (*intersymbol interference*, ISI) (LATHI e DING, 2012) e é utilizado no transmissor para limitar a banda do sinal. O RCF limita a banda do sinal $M[n]$ de acordo com o fator de decaimento (*roll-off*), r:

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

sendo R_{ry} a taxa de transmissão de símbolos do sinal

A função “IFFT” corresponde à transformada rápida de Fourier inversa (*inverse fast Fourier transform*, IFFT). A IFFT é responsável por passar o sinal do domínio da frequência para o domínio do tempo.

O submódulo chamado de “ADC” corresponde ao Conversor Análogico Digital (*Digital to Analog Conversion*, ADC). O submódulo “ADC” é responsável por realizar a discretização das amplitudes do sinal de acordo com o número de níveis estabelecidos no submódulo “Parâmetros”, simulando a conversão do sinal de analógico para digital.

2.1.2. Canal ruidoso

O canal ruidoso foi implementado no *software* Matlab para representar a introdução de AWGN aos sinais. O cálculo e a descrição da potência de ruído segue sendo a mesma descrita em (SANTOS, 2020), pois utiliza-se a mesma implementação responsável pela adição do ruído AWGN aos sinais.

2.1.3. Receptor

O sinal, assim que chega ao receptor, é demapeado e estimada a BER. O submódulo “Demapeador” é usado para converter os símbolos recebidos em uma sequência de bits. Para avaliação da BER supõe-se que o sinal transmitido utilizou a codificação de Gray. Essa codificação impõe a ocorrência de apenas um bit distinto entre símbolos adjacentes e, consequentemente, provê uma BER menor do que de outras codificações. Nesse submódulo, a BER é estimada pelas 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 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 bit errados detectados pode ser muito baixo e poucos confiáveis em termos estatísticos. O contador de erros retorna a BER e a taxa de símbolos de erro (*Symbol Error Rate*, 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. As fórmulas e procedimento de cálculo implementado no código são baseadas teóricamente em (LATHI e DING, 2012) e

também são assumidas as mesmas descrições e cáculos de (ABBADE *et al.*, 2020) e (SANTOS, 2020).

Quando as taxas de erro de bits são suficientemente altas (maiores que $0{,}003$) 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 fórmulas de distribuição gaussiana (SANTOS, 2020). Durante o trabalho foi considerado se de fato a distribuição de pontos nas constelações era aproximadamente gaussiana, justificando a utilização das fórmulas consideradas para estimativa da BER.

A dependência da BER com a SNR é útil para comparar as qualidades do sinal transmitido e recuperado. A fórmula da SNR é dada por (2):

$$SNR = \frac{P_s}{P_r}, \tag{2}$$

sendo P_s e P_r respectivamente a potência do sinal e a potência do ruído após um filtro retangular utilizado no receptor.

A SNR em dB:

$$SNR[dB] = (10)[log_{10}\left(\frac{P_s}{P_r}\right)] \tag{3}$$

2.2. Técnicas de criptografias e aplicações

A seguir serão descritas as técnicas de criptografias utilizadas neste trabalho. As técnicas desenvolvidas serão descritas separadamente com objetivo de simplificar a explicação de cada técnica utilizada no desenvolvimento do código atual. A Seção 2.2.1 descreve as funções “Codificação de Fase” e “Decodifiação de Fase” referente a técnica de criptografia de fase; a Seção 2.2.2 aborda as funções “Embaralhador” e “Desembaralhador” referente a técnica de criptografia de embaralhamento; a Seção 2.2.3 descreve sobre as funções “Adição de Amplitudes Falsas”, “Remoção de Amplitudes Falsas” e “Parâmetros 2” referente as novas melhorias de transmissão de dois sinais com taxas distintas; a Seção 2.2.4 descreve sobre sinalizações diferentes e a Seção 2.2.5 descreve sobre a chave dinâmica.

2.2.1. Descrição da técnica de criptografia de fase

No estudo realizado durante o trabalho (ABBADE; NOGUEIRA *et al.*, 2020) percebeu-se que a junção das técnicas de criptografias de embaralhamento com a de

codificação de fase e atraso se tornavam mais seguras considerando uma amostra por fatia. No entanto, quando há apenas uma amostra por fatia, aplicar uma diferença de fase e um atraso equivale a aplicar uma única diferença de fase a essa amostra. Por isso, considera-se neste trabalho apenas a técnica de codificação espectral de fase em DSP (*spectral phase and delay encoding*, SPE-DSP).

A função "Chave Fase" localizada no módulo "Geração de Chaves Criptográficas" gera n_s fatias espectrais e a seguir sorteia-se a partir de uma distribuição uniforme de valores de fase, φ_i, que serão usados para encriptar a i-ésima fatia. O conjunto de fases é armazenados em uma matriz, sendo a chave criptográfica chamada de "Chave Fase" no diagrama da Figura 4.

A função "Codificação de Fase" realiza no domínio da frequência a encriptação dos sinais aplicando a técnica SPE em banda base a partir da "Chave Fase". Essa encriptração é feita multiplicando-se as componentes espectrais da i-ésima fatia por $exp(j\varphi_i)$.

O sinal é decodificado na função "Decodificador de Fase" a partir da leitura da "Chave Fase", que é utilizada para desencriptar as fatias espectrais multiplicando-as por $\{\exp(j\varphi_i)\}^*$ = exp $(-j\varphi_i)$. Na ausência de ruído e de distorções do sinal, os valores de fase originais são retomados após as fatias espectrais dos sinais serem descriptografadas.

2.2.2. Descrição da técnica de criptografia de embaralhamento

Na técnica de embaralhamento é necessário que, no mínimo, sejam gerados e transmitidos dois sinais. A quantidade máxima de sinais é ilimitada, porém a avaliação em trabalhos e artigos publicados foi de até 4 sinais sendo gerados, embaralhados, transmitidos e recuperados (ABBADE; NOGUEIRA *et al*., 2020). A explicação da técnica de embaralhemento neste trabalho será feita considerando apenas 2 sinais.

A "Chave Embaralhador" é gerada na função "Chave Embaralhador" localizada no módulo "Geração das Chaves Criptográficas". As posições que cada fatia espectral irá assumir são geradas de forma aleatória. As posições de troca das fatias espectrais para o embaralhamento entre os sinais são armazenadas em um em uma matriz, chamada de "Chave Embaralhadora". A "Chave Embaralhadora" é a chave criptográfica da técnica de embaralhamento (ABBADE; NOGUEIRA *et al*., 2020) e (NOGUEIRA, 2019).

A função “Embaralhador” aplica o embaralhamento de componentes espectrais entre os sinais gerados a partir da “Chave Embaralhadora”. Se o número de sinais é 2, então, são embaralhados os componentes espectrais entre o sinal $M_1[n]$ e o sinal $M_2[n]$.

O submódulo “Desembaralhador” recebe os sinais embaralhados e a partir da “Chave Embaralhadora” são desembaralhadas as fatias espectrais entre os sinais. Cada fatia espectral é retornada a sua posição e ao sinal original.

2.2.3. Descrição da aplicação à sinais com taxas transmissão distintas

A técnica de transmissão de sinais com taxas distintas possui duas versões. A primeira e segunda versão considera-se a geração, transmissão e recepção de dois sinais. As duas versões serão descritas nós paragráfos seguir.

Os sinais na primeira versão são gerados com os parâmetros de taxas de transmissão de símbolos e largura de banda distintas e transmitidos pelo canal com taxas e largura de banda diferentes. O único parâmetro alterado no código é a taxa de transmissão de símbolos. Os sinais são transmitidos com taxas diferentes sem nenhuma alteração no número de amostras. A transmissão realizada dessa forma possui desvantagem de que se há um intruso na rede é facil associar a diferença dos sinais, pois possuem larguras de banda diferentes.

Os sinais na segunda versão 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. Essa segunda versão aumenta a segurança de dados, pois durante a transmisão dos sinais, caso haja algum intruso, esse não consegue distinguir a diferença entre os dois sinais. A desvantagem é que como cada sinal possui características particulares (número de amostras, número de símbolos, taxa de transmissão de símbolos e largura de banda) foi necessário criar uma nova função chamada no diagrama da Figura 4 de “Parâmetros 2” para que os parâmetros que fossem totalmente diferentes de um sinal em comparação ao outro fossem atribuídos de forma correta ao longo do código. Esses parâmetros quando necessários, são carregados de acordo com o sinal a ser tratado.

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, portanto, não é aplicado nehuma técnica diferente. Porém o sinal que possui menor taxa de transmissão de símbolo e menor número de amostras requer a realização de alterações para que

assuma, durante a transmissão pelo canal, mesmo valor da taxa de transmissão e o mesmo número de amostras do outro sinal.

A função “Mapeador” gera os dois sinais. O sinal com taxa de transmissão menor será passado pelo submódulo “Adição de Amplitudes Falsas”. A explicação da técnica será 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 $m_1[n]$:
   a. 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. O sinal $m_1[n]$ é dividido em eixo I e eixo Q e são selecionados os pontos de amostragem. 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. Exemplo considerando o sinal $m_1[n]$ de tamanho 10 amostras com modulação em 16-QAM 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. $m_{1_{falso\_I}}[n]$ = [1 1 3 -1 3 1 -3 -3 1 -1 3 3 1 -3]
   ii. $m_{1_{falso\_Q}}[n]$ = [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 da Figura 4 de “Chave Amplitudes Originais”.
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 $m_{1_{falso\_I}}[n]$ e $m_{2_{falso\_Q}}[n]$ são combinados e é gerado o novo sinal $m_{1_{falso}}[n]$:

a. $m_{1_{falso}}[n]$ = [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 $m_1[n]$.

2.2.4. Descrição da aplicação de sinais com sinalizações diferentes

A função "Mapeador" é responsável por aplicar a técnica de sinalizações diferentes. O *software* foi alterado na forma com que os parâmetros são carregados já visto na Subseção 2.2.3. A alocação de uma nova função, chamada de "Parâmetros 2" foi necessária para a atribuição dos parâmetros corretos para a geração dos sinais com o tipo de sinalização desejada sendo 2-PAM para a modulação QPSK e 4-PAM para a modulação 16-QAM. Nessa função, quando carregada ao longo do código, se pode ter acesso aos parâmetros do sinal 1 ou do sinal 2 e, assim, é possível atribuir todos os parâmetros particulares de cada sinal de uma única vez. A nova função "Parâmetros 2" possibilitou no momento da geração dos sinais no "Mapeador" atribuir os parâmetros da sinalização desejada, sendo possível gerar sinais com sinalizações diferentes.

2.2.5. Descrição do algoritmo de chave dinâmica

A descrição completa da DK é encontrada em (NGO, 2010). A explicação da geração da chave dinâmica para este trabalho foi realizada em (SANTOS, 2020). A explicação sobre a geração da DK em blocos é baseada na Figura 5. 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 pode ser realizada por meio da distribuições de chave quântica (*quantum key distribuition*, QKD) via satélites (Liao et al., 2017).
2. "Alice" e "Bob" geram a chave semente, K_s, a partir de uma função XOR entre as chaves K_t e K_i:

$$K_s = K_t \oplus K_i \tag{10}$$

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:

$$DK_1 = f(K_s, K_t) \tag{12}$$

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

$$DK_2 = f(K_s, K_t) \tag{13}$$

   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:

$$DK_n = f(K_s, K_{(n-1)}) \tag{14}$$

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

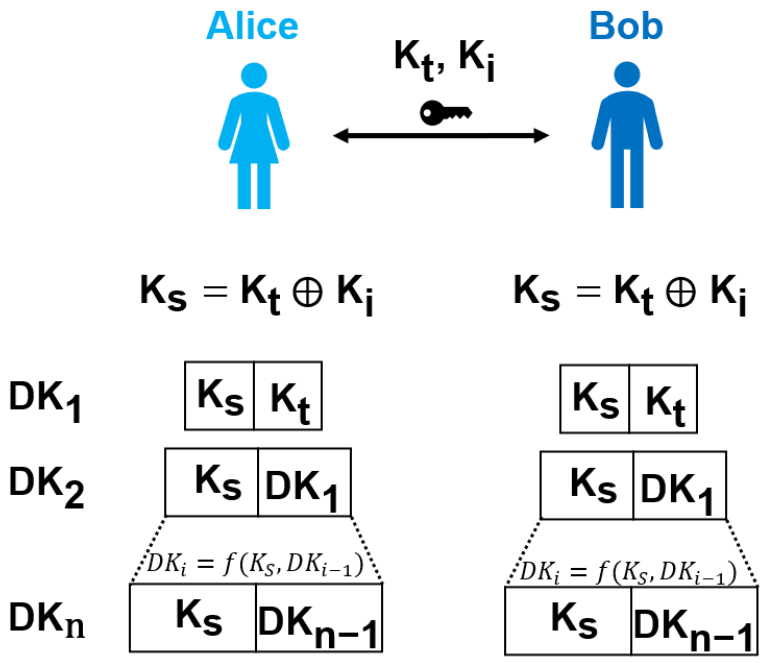

Figura 5 – Esquemático iustrativo e simplificado da geração de chaves dinâmicas.

A função de mão única tém aplicação no sentido direto de sua operação, porém no sentido inverso é relativamente difícil calcular. Nesse trabalho, escolheu-se como função de mão única a função de *whirlpool* (SOUZA *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.

O diagrama da Figura 4 ilustra a organização do código baseado no algoritmo DK e, a Figura 7 e Figura 7 são diagramas ilustrativos para auxiliar na explicação da DK implementada no código. Os submódulos “Geração de Chaves Criptográficas”, “Geração e Critptografia de Sinais em Blocos” e “Descriptografia de Sinais em Blocos” possuem uma iteração (“l*oop*”), que é repetida de acordo com a quantidade de blocos definida, ou seja, a quantidade de partes que o sinal irá possuir. A quantidade de blocos é definida no submódulo “Parâmetros”.

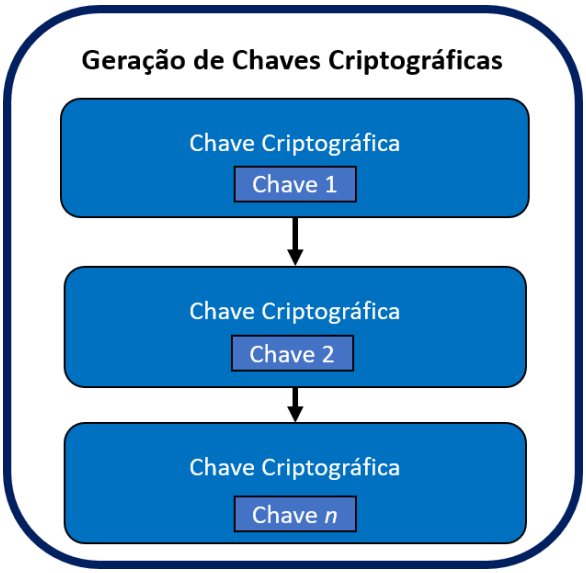

Figura 6 - Diagrama representativo sobre a geração de chaves criptográficas a partir da chave dinâmica. Fonte: Autoria própria.

O submódulo “Geração de Sinais e Criptografia de Sinais em Blocos” é responsável por realizar a geração de sinais em blocos e aplicar as criptografias no bloco correspondente à chave criptográfica. Os blocos, ainda nesse submódulo, são concatenados, ou seja, é gerado o sinal completo na função “Agrupamentos de Blocos”. Os números que identificam os blocos estão contidos na matriz que contém o sinal para que no receptor seja possível realizar a divisão e a descriptografia do sinal bloco por

bloco. Como exemplo, se o código é programado para número de blocos igual a 2 ($n = 2$). O primeiro submódulo “Geração de Chaves Criptográficas” realiza a geração de duas chaves criptográficas. O diagrama na Figura 6 ilustra a implementação realizada no código referente a geração das chaves criptográficas.

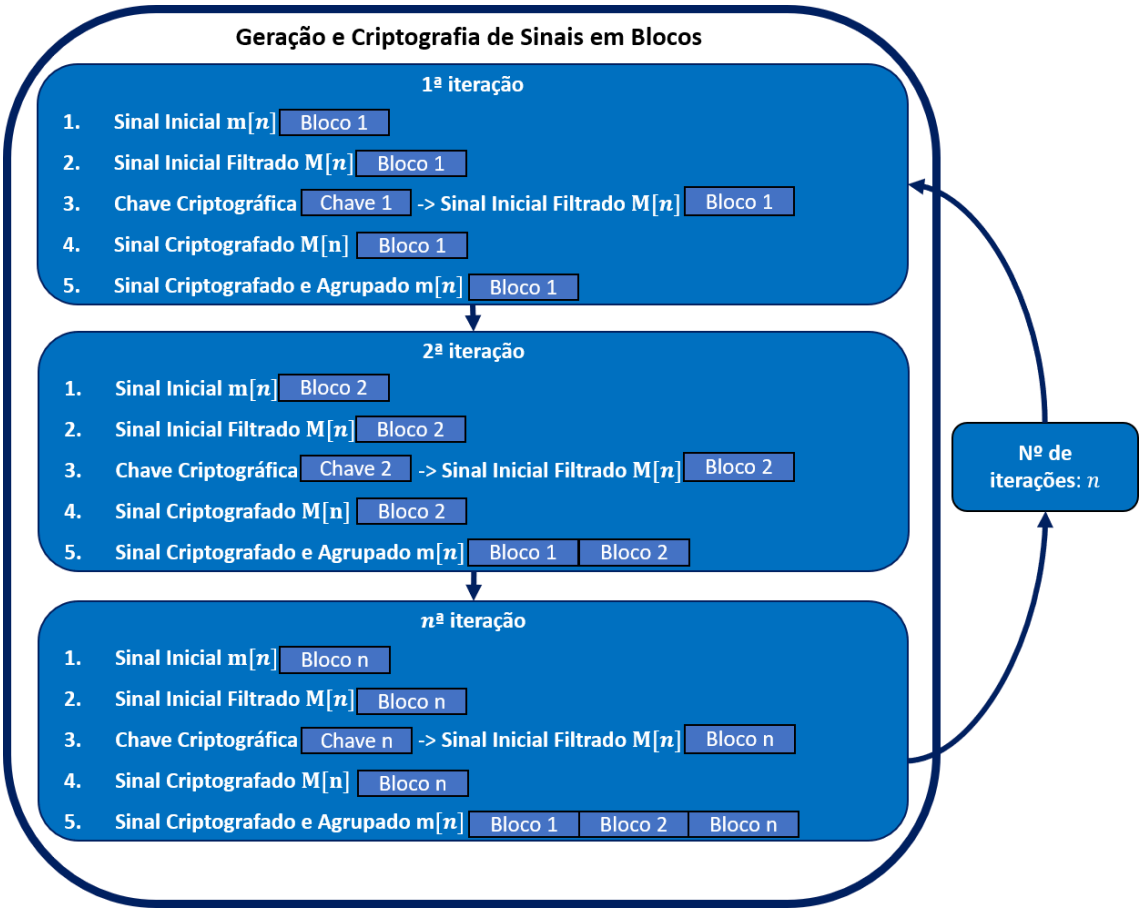

Figura 7 - Diagrama representativo sobre a geração dos sinais criptografados a partir da chave cinâmica. Fonte: Autoria própria.

No submódulo “Geração e Criptografia de Sinais em Blocos” é gerado o sinal em duas iterações, considerando $n = 2$. Em cada bloco gerado do sinal é aplicado a criptografia de acordo com o chave correspondente. Exemplo, a primeira chave criptográfica é aplicado ao primeiro bloco do sinal gerado. A segunda chave criptográfica é aplicada ao segundo bloco do sinal gerado. A Figura 7 ilustra a implementação realizada no código para a geração e criptografia dos sinais em blocos.

3. RESULTADOS

Os resultados e avaliações das melhorias desenvolvidas neste trabalho serão descritas e apresentadas neste Capítulo, que será dividido em duas Seções. A primeira Seção, 3.1, apresenta os resultados das constelações e dos espectros dos sinais gerados, criptografados, transmitidos por um canal AWGN e, posteriormente, descriptografados e recuperados. A técnica de criptografia utilizada é SPE-SS-DSP com DK aplicadas a sinais com taxas de transmissão distintas e sinalizações diferentes. A Subseção 3.1.1 aborda os resultados em relação a primeira versão de taxas de transmissão distintas, enquanto que a Subseção 3.1.2 aborda os resultados em relação a segunda versão de taxas de transmissão distintas. Ambas as Subseções, 3.1.1 e 3.1.2, apresentam os espectros e constelações para uma SNR alta e apresentam os espectros e constelações para uma SNR baixa próxima do limite da FEC. Segundo a recomendação da G.975.1 (2004) do ITU (TYCHOPOULOS; KOUFOPAULOU; TOMKOS, 2006), o valor da BER para o limite da FEC padronizada é de 2.10^{-3}. 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 conseguir uma recepção livres de erros quando aplicado o algoritmo da FEC.

Os resultados da BER e SNR são apresentados na Seção 3.2. A ordem de simulação e de comparação das técnicas de criptografias e melhorias foi: SPE-DSP; SS-DSP; SPE-SS-DSP; SPE-SS-DSP com taxas de transmissão de sinais distintas; SPE-SS-DSP com taxas de transmissão distintas e sinalizações diferentes; SPE-SS-DSP com taxas de transmissão distintas, sinalizações diferentes e chave dinâmica. A cada curva obtida durante as simulações seguiu essa ordem de comparação para verificar a geração ou não de penalidades aos sinais transmitidos e recuperados. A Subseção 3.2.1 consta os resultados da primeira versão de taxas de transmissão distintas, enquanto que a Subseção 3.2.2 consta os resultados da segunda versão de taxas de transmissão distintas.

3.1. Análise de propagação pelo canal AWGN

O *software* KryptoSJ contém a implementação da chave dinâmica e como os sinais são gerados em blocos, então em cada bloco do sinal 1 é gerado um sinal QPSK com 2 bits por símbolo e taxa de símbolo igual a 28 GBaud. O fator de *roll-off* do RCF é igual a 0,02, logo, a banda codificada é de 14,28 GBaud em banda base. As PRBS utilizadas possuem um comprimento de 1024 bits para uma sequência de bits associada ao eixo I e eixo Q. Enquanto que para o sinal 2 é gerado um sinal 16-QAM com 4 bits por símbolo

e taxa de símbolo igual a 42 GBaud. A banda codificada é de 21,42 GBaud em banda base. As PRBS utilizadas possuem um comprimento de 1024 bits para uma sequência de bits associada ao eixo I e eixo Q considerando a primeira técnica de taxas de transmissão distintas e um comprimento de 2048 bits para um sequência de bits associada ao eixo I e Q considerando a segunda técnica de taxas de transmissão distintas.

Observa-se que considerado a aplicação da segunda técnica de taxas de transmissão distintas ao sinal 1, os comprimentos das sequências se igualam ao do sinal 2. A taxa de símbolo do sinal 1 passa a ser de 42 Gbaud, a banda codificada de 21,42 GBaud em banda base e um comprimento de 2048 para uma sequência de bits associada ao eixo I e Q.

O total de blocos considerado nas simulações foi de 32. Cada sinal, portanto, possui 32 blocos que são criptografadas no módulo "Transmissor" e descriptografadas no módulo "Receptor". O sinal 1, após concatenados os 32 blocos, possui comprimento da palavra PRBS de 32768 para uma sequência de bits associada ao eixo I e eixo Q. O sinal 2, após concatenados os 32 blocos, possui comprimento da palavra PRBS de 32768 para uma sequência de bits associada ao eixo I e eixo Q considerando a primeira técnica de taxas de transmissão distintas e um comprimento de 65536 bits para uma sequência de bits associada ao eixo I e eixo Q considerando a segunda técnica de taxas de transmissão distintas.

Observa-se que considerado a aplicação da segunda versão de taxas de transmissão distintas ao sinal 1, após os sinais 1 e 2 serem concatenados em 32 blocos, o comprimento das sequências se igualam ao do sinal 2. A taxa de símbolo do sinal 1 passa a ser de 42 Gbaud, a banda codificada de 21,42 GBaud em banda base e o comprimento de 65536 para uma sequência de bits associada ao eixo I e Q.

As simulações em que os sinais são criptografados foram utilizadas apenas uma amostra por fatia para promover maior robustez de ataques de força bruta como já abordado em (NOGUEIRA, 2019).

Foram obtidos os espectros e as constelações dos sinais 1 e 2 em quatro etapas:

1) Na primeira etapa foram obtidos os sinais 1 e 2 gerados pelo submódulo "Mapeador". As siglas que identificam os sinais nessa etapa são m_1 e M_1 para o primeiro sinal e m_2 e M_2 para o segundo sinal.

2) Na segunda etapa foram obtidos os sinais 1 e 2 após o submódulo “Geração e Criptogrfia de Sinais em Blocos”, ou seja, após os sinais serem criptografados. As siglas que identificam os sinais nessa etapa são c_1 e C_1 para o primeiro sinal e c_2 e C_2 para o segundo sinal.
3) Na terceira etapa foram obtidos os sinais 1 e 2 após o módulo “Canal Ruidoso”, ou seja, após os sinais serem transmitidos. As siglas que identificam os sinais nessa etapa são r_1 e R_1 para o primeiro sinal e r_2 e R_2 para o segundo sinal.
4) Na quarta etapa foram obtidos os sinais 1 e 2 recuperados após o submódulo “Demapeador”. As siglas que identificam os sinais nessa etapa são d_1 e D_1 para o primeiro sinal e d_2 e D_2 para o segundo sinal.

3.1.1. Aplicação da primeira versão de taxas de transmissão distintas

Os gráficos das constelações e espectros são apresentados na Figura 8 e Figura 9 respectivamente considerando uma SNR muito alta:

$$\lim_{P_r \to 0} SNR = \infty$$

Na Figura 8(a) e Figura 8(b) são mostradas as constelações dos sinais complexos de entrada gerados em banda base no módulo “Mapeador” sem estarem criptografados e com os pontos bem definidos nas amplitudes correspondentes com o esquema de sinalização utilizada. Na Figura 8(c) e Figura 8(d) são mostrados os sinais criptografados e agrupados após o submódulo “Geração e Criptografia de Sinais em Bloco” e possuem distribuição de amplitude aproximadamente gaussianas nos eixos I e Q. Na Figura 8(e) e Figura 8(f) é mostrado os sinais transmitidos e com ruído após o módulo “Canal Ruidoso”. O ruído adicionado é muito baixo, então não gerou diferenças nas distribuições de pontos entre a Figura 8(c) e Figura 8(e) e entre a Figura 8(d) e Figura 8(f). Na Figura 8(g) e Figura 8(h) são mostrados os sinais descriptografados e recuperados após o submódulo “Descriptografia de Sinais em Bloco”. Os pontos novamente estão bem definidos nas amplitudes correspondentes ao esquema de sinalização utilizada, possuindo uma BER nula.

Na Figura 9(a) e Figura 9(b) são apresentados os espectros dos sinais complexos gerados em banda base no módulo “Mapeador” sem estarem criptografados e sem terem passado pelo RCF. Já nas Figura 9(c) e Figura 9(d) são mostrados os sinais criptografados após o módulo “Geração e Criptografia de Sinais em Bloco”. Após esse submódulo, os 32 blocos dos sinais gerados foram concatenados no domínio do tempo e após a FFT foi

obtido os sinais no domínio da frequência e, posteriormente, os espectros de cada sinal. Os espectros dos sinais transmitidos e com ruído após o módulo “Canal Ruidoso” são apresentados na Figura 9(e) e Figura 9(f). Como a potência do ruído adicionado é muito baixa, não gerou diferença de amplitudes das componentes espectrais entre a Figura 9(c) e Figura 9(e) e entre a Figura 9(d) e Figura 9(f). Por fim, na Figura 9(g) e Figura 9(h) são mostrados os sinais recuperados após o último submódulo “RCF” no módulo “Receptor”. Após o módulo “Descriptografia de Sinais em Blocos” os 32 blocos dos sinais 1 e 2 foram concatenados no domínio do tempo e após a FFT foi obtido os sinais no domínio da frequência. Os sinais após concatenados e já no domínio da frequência passaram pelo último submódulo “RCF” do módulo “Receptor” para limitar a banda e obter os sinais recuperados, e posteriormente, os espectros de cada sinal.

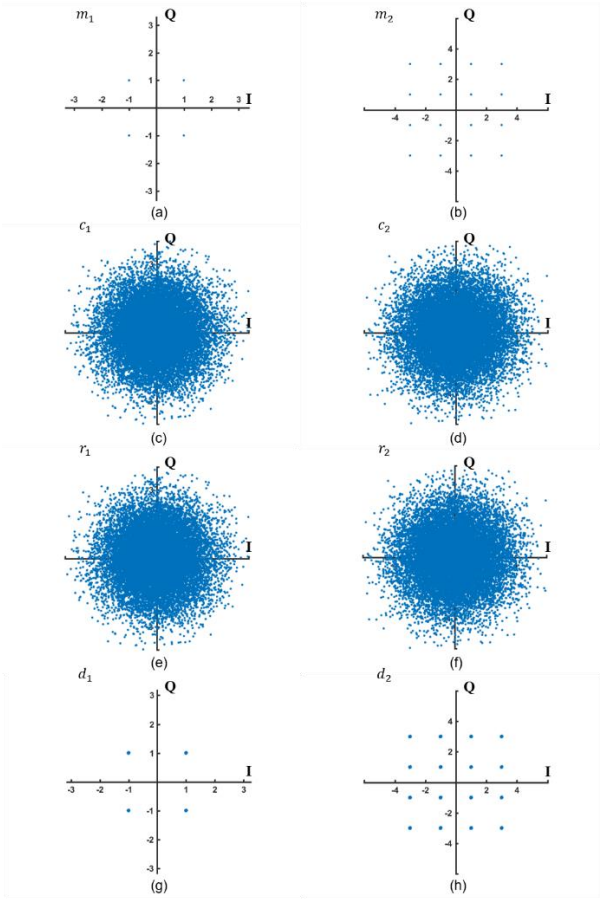

Figura 8 - Constelações obtidas com alta SNR e com aplicação da primeira versão de taxas de transmissão distintas para o (a) primeiro sinal de entrada, (b) segundo sinal de entrada, (c) primeiro sinal criptografado, (d) segundo sinal criptografado, (e) primeiro sinal criptografado com ruído, (f) segundo sinal criptografado e com adição de ruído, (g) primeiro sinal descriptografado e recuperado e, (h) segundo sinal descriptografado e recuperado. Fonte: Autoria própria.

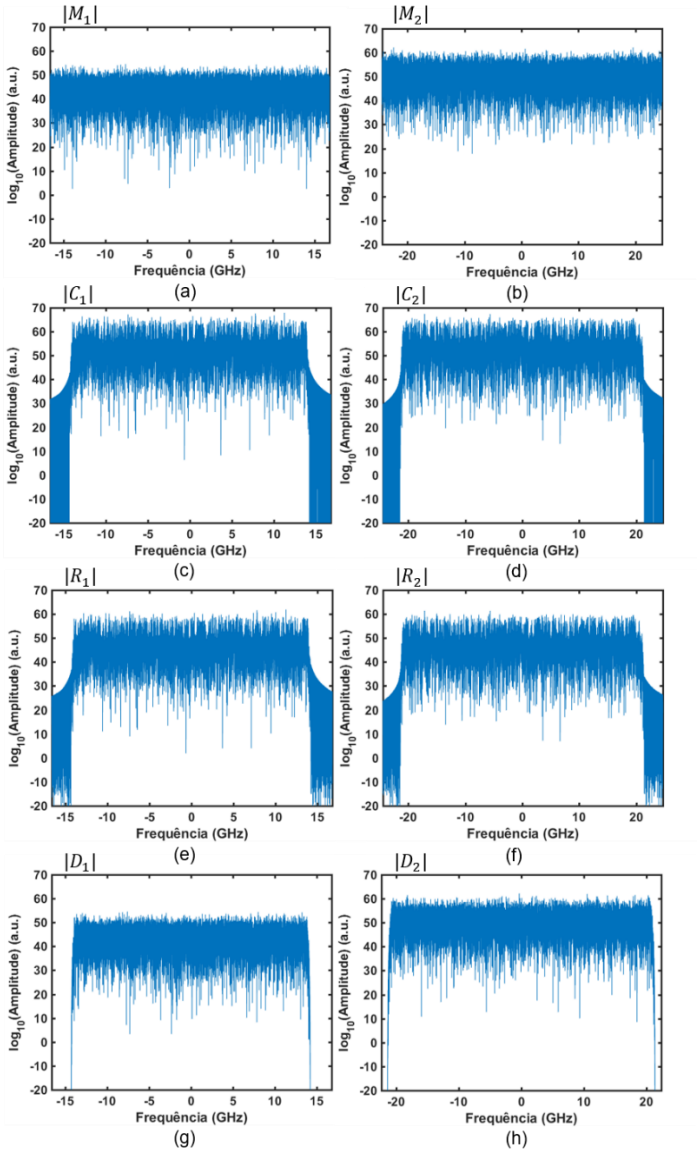

Figura 9- Espectros de amplitude com alta SNR e com aplicação da primeira versão de taxas de transmissão distintas para o (a) primeiro sinal de entrado, (b) segundo sinal de entrada, (c) primeiro sinal criptografado, (d) segundo sinal criptografado, (e) primeiro sinal criptografado e com ruído, (f) segundo sinal criptografado e com adição de ruído, (g) primeiro sinal descriptografado e recuperado e, (h) segundo sinal descriptografado e recuperado. Fonte: Autoria própria.

Os gráficos das constelações e espectros são apresentados nas Figura 10 e Figura 11 respectivamente, considerando um valor de SNR próximo ao limite da FEC. Na Figura 10 e Figura 11 seguem as mesmas análises e descrições realizadas para a Figura 8 e Figura 9, porém com a adição de uma potência de ruído maior. A adição de uma potência de ruído maior resulta na distribuição de pontos diferentes entre a constelação do primeiro sinal criptografado da Figura 10(c) e a constelação do primeiro sinal criptografado e com

ruído da Figura 10(e), assim como, resulta na distribuição de pontos diferentes entre a constelação do segundo sinal criptografado da Figura 10(d) em relação a constelação do segundo sinal criptografado e com ruído da Figura 10(f). Na Figura 10(g) e Figura 10(h) são mostradas as constelações com uma distribuição de pontos gaussiana centrada nos pontos de amplitudes correspondentes aos esquemas de sinalizações utilizadas, pois a BER está próxima do valor da FEC. A adição de uma potência de ruído maior resulta em amplitudes de componentes espectrais diferentes entre o primeiro sinal criptografado da Figura *11*(c) e o primeiro sinal criptografado com ruído da Figura *11*(e) e resulta em amplitudes de componentes espectrais diferentes entre o segundo sinal criptografado da Figura *11*(d) e o segundo sinal criptografado com ruído da Figura *11*(f).

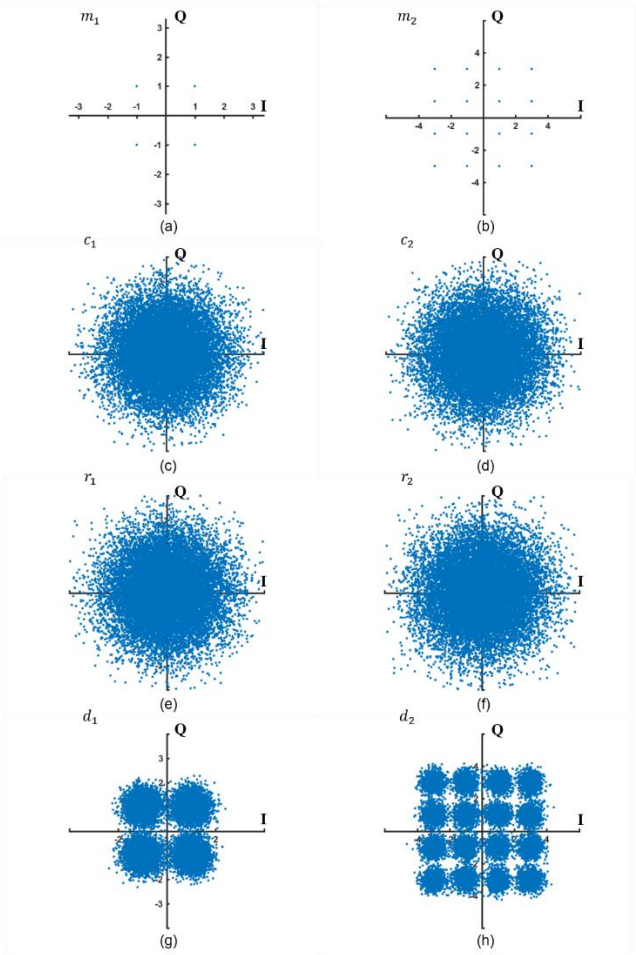

Figura 10 - Constelações obtidas com baixa SNR e com aplicação da primeira versão de taxas de transmissão distintas para o (a) primeiro sinal de entrada, (b) segundo sinal de entrada, (c) primeiro sinal criptografado, (d) segundo sinal criptografado, (e) primeiro sinal criptografado com ruído, (f) segundo sinal criptografado e com adição de ruído, (g) primeiro sinal descriptografado e recuperado e, (h) segundo sinal descriptografado e recuperado. Fonte: Autoria própria.

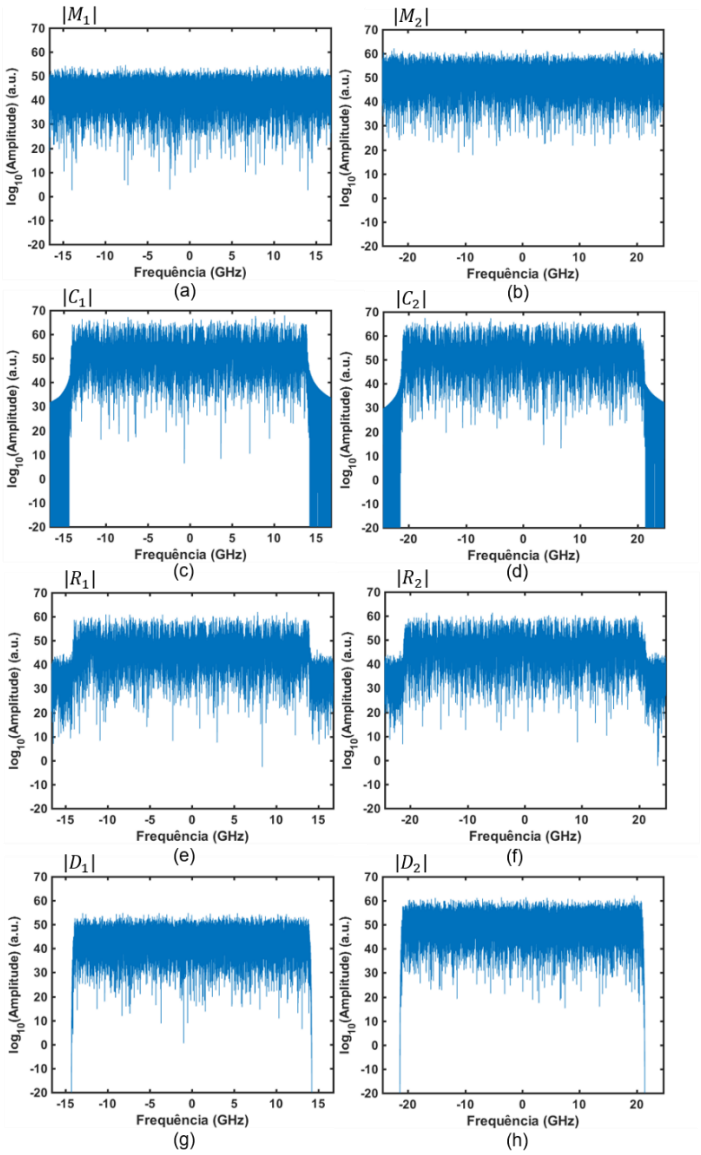

Figura 11 - Espectros de amplitude com baixa SNR e com aplicação da primeira versão de taxas de transmissão distintas para o (a) primeiro sinal de entrado, (b) segundo sinal de entrada, (c) primeiro sinal criptografado, (d) segundo sinal criptografado, (e) primeiro sinal criptografado e com ruído, (f) segundo sinal criptografado e com adição de ruído, (g) primeiro sinal descriptografado e recuperado e, (h) segundo sinal descriptografado e recuperado. Fonte: Autoria própria.

As diferenças da taxa de transmissão e largura de banda entre os sinais 1 e 2, durante a transmissão, não são identificadas no domínio do tempo com base nas constelações da Figura 8(e), Figura 8(f), Figura 10(e) e Figura 10(f). Porém, com a diferença da largura de banda, em análise no domínio da frequência, fica evidente que o sinal 1 possui menor largura de banda (14,28 GHz) e menor taxa de transmissão (28 GBaud) do que o sinal 2, que possui maior largura de banda (21,42 GHz) e maior taxa de

transmissão (42 GBaud) com base na Figura 9(e), Figura 9(f), Figura 11(e) e Figura 11(f). O intruso, caso houver, se realizar uma análise espectral conseguirá identificar a diferença entre os sinais, deixando-os mais vuneráveis à ataques.

3.1.2. Aplicação da segunda versão de taxas de transmissão distintas

Os gráficos das constelações e espectros são apresentados na Figura 12 e Figura 13 respectivamente, considerando uma SNR muito alta:

$$\lim_{P_r \to 0} SNR = \infty$$

Na Figura 14 e Figura 15 são apresentados os gráficos das constelações e espectros respectivamente, considerando uma SNR próxima do limite da FEC. A Subseção 3.1.2 possui os resultados com descrição e ordem semelhantes da Subseção 3.1.1. Os resultados são muito parecidos com o da primeira versão, com diferenças de que os sinais, nesse caso, são transmitidos com taxas de transmissão e largura de banda iguais.

As constelações apresentadas na Figura 12 ficaram muito semelhantes as constelações da Figura 8 com pontos bem definidos nas amplitudes correspondentes ao tipo de sinalização utilizada. Com exceções das constelações dos sinais criptografados com ruído, que possuem distribuição de pontos diferentes comparando a Figura 8(c) com a Figura 12(c), Figura 8(d) com a Figura 12(d), Figura 8(e) com a Figura 12(e) e Figura 8(f) com a Figura 12(f). Os espectros dos sinais criptografados da Figura 13(c) e Figura 13(d) possuem mesma taxa de transmissão e largura de banda, diferentes dos sinais criptografados com aplicação da primeira versão de taxas transmissão distintas referente a Figura 9(c) e Figura 9(d).

Na Figura 14 e Figura 15 são apresentadas as constelações e espectros respectivamente com uma potência de ruído maior (SNR próxima ao limite da FEC). As constelações dos sinais de entrada da Figura 14 ficaram muito semelhantes as constelações dos sinais de entrada da Figura 10 com pontos bem definidos nas amplitudes correspondentes ao tipo de sinalização utilizada. Como a SNR é considerada próxima do limite da FEC e o ruído do canal é significativo, os sinais possuem distribuição de pontos diferentes antes e depois de transmitidos pelo canal, comparando a Figura 14(c) com a Figura 10(c), Figura 14(d) com a Figura 10(d), Figura 14(e) com a Figura 10(e) e Figura 14(f) com a Figura 10(f) pode-se observar essas diferenças. As contelações do sinais descriptografados e recuperados possuiram uma penalidade um pouco maior comparados as constelações da Figura 14(g) com a Figura 10(g) e a Figura 14(h) com a Figura 10(h).

Essa diferença não causou alteração significativa nos valores da BER, que mantiveram-se na mesma ordem de grandeza de 10^{-3} comparando a primeira e a segunda versão de taxas de transmissão distintas. Os espectros dos sinais criptografados da Figura 15(c) e Figura 15(d) possuem mesma taxa de transmissão e largura de banda, o que diferencia da primeira técnica de taxas de transmissão distintas referente a Figura 11(c) e Figura 11(d), que possuem taxa de transmissão e largura de banda diferentes.

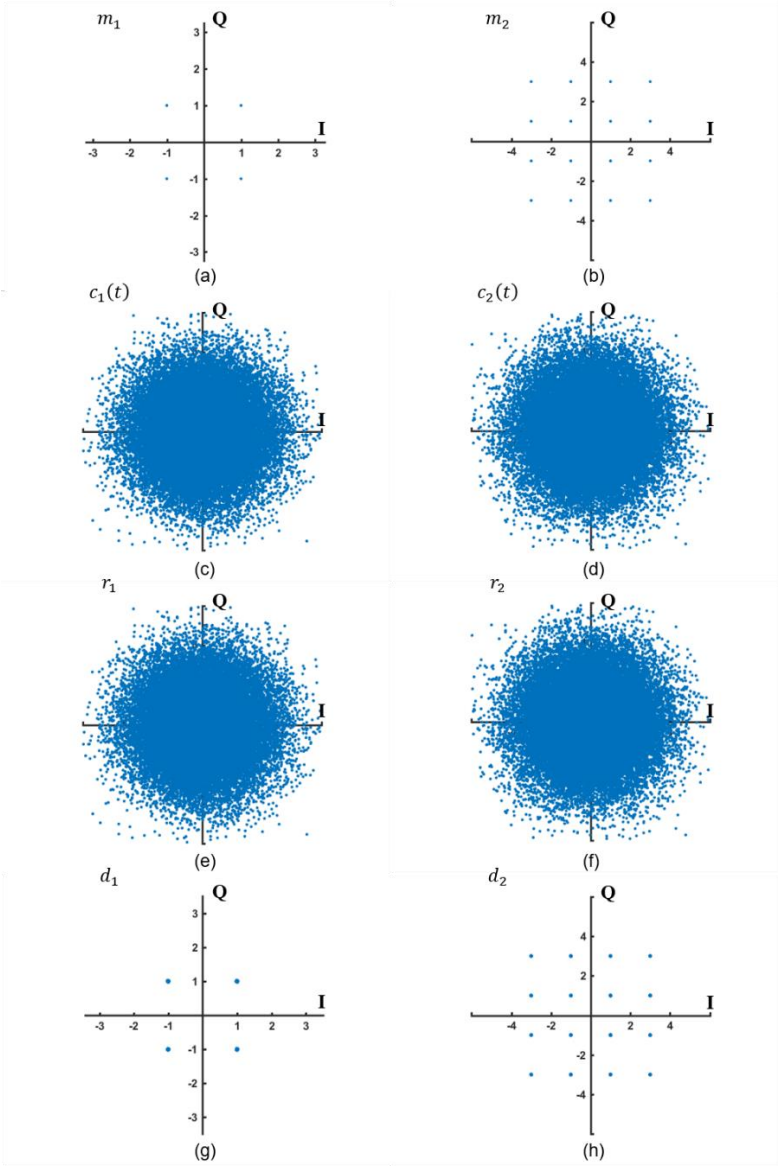

Figura 12 – Constelações obtidas com alta SNR e com aplicação da segunda versão de taxas de transmissão distintas para o (a) primeiro sinal de entrada, (b) segundo sinal de entrada, (c) primeiro sinal criptografado, (d) segundo sinal criptografado, (e) primeiro sinal criptografado com ruído, (f) segundo sinal criptografado e com adição de ruído, (g) primeiro sinal descriptografado e recuperado e, (h) segundo sinal descriptografado e recuperado. Fonte: Autoria própria.

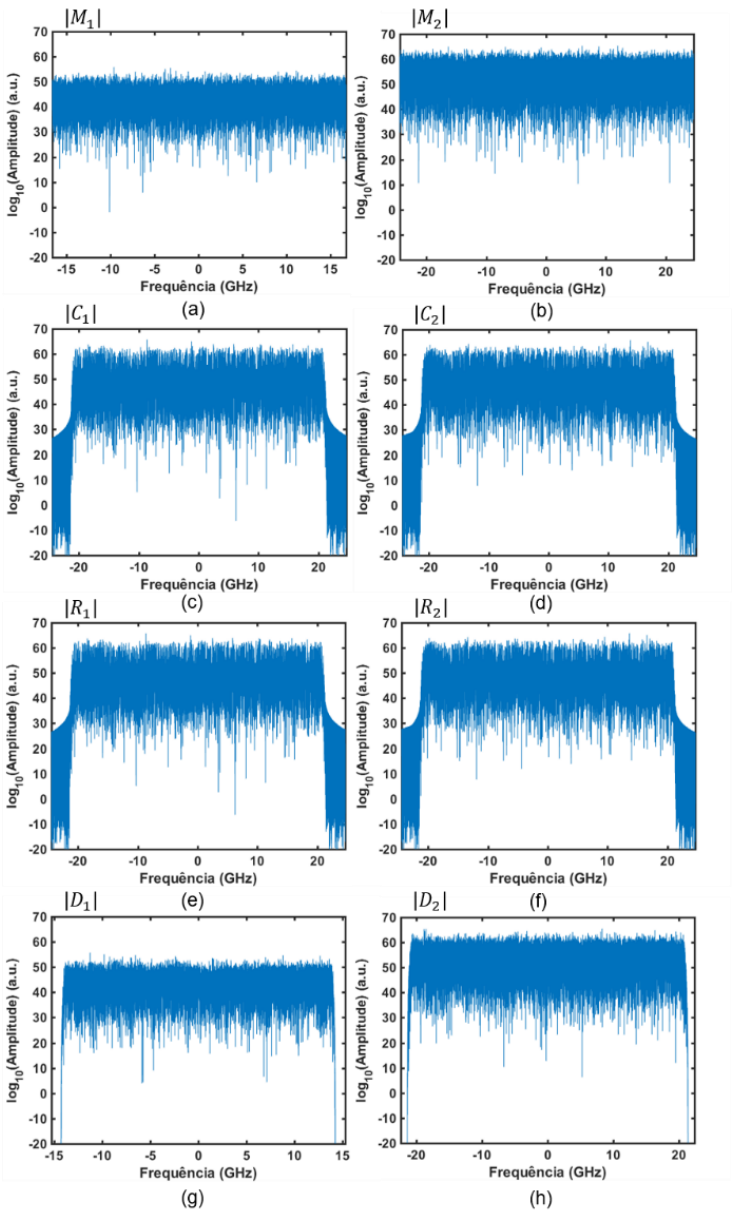

Figura 13 - Espectros de amplitude com alta SNR e com aplicação da segunda versão de taxas de transmissão distintas para o (a) primeiro sinal de entrado, (b) segundo sinal de entrada, (c) primeiro sinal criptografado, (d) segundo sinal criptografado, (e) primeiro sinal criptografado e com ruído, (f) segundo sinal criptografado e com adição de ruído, (g) primeiro sinal descriptografado e recuperado e, (h) segundo sinal descriptografado e recuperado. Fonte: Autoria própria.

As diferenças da taxa de transmissão e largura de banda entre os sinais 1 e 2 no domínio do tempo não são identificadas com base na Figura 12(e), Figura 12(f), Figura 14(e) e Figura 14(f). Nessa versão de taxas de transmissão distintas, os sinais são transmitidos com taxas e largura de banda iguais. Dessa forma, não é possível identificar, durante a transmissão, qual sinal foi gerado com menor largura de banda e menor taxa de

transmissão e qual sinal foi gerado com maior largura de banda e menor taxa de transmissão com base nos espectros da Figura 13(e), Figura 13(f), Figura 15(e) e Figura 15(f). O intruso, caso houver, se obter os espectros dos sinais transmitidos não conseguirá identificar qual é o sinal 1 e o sinal 2, deixando-os mais seguros a ataques. Além de que, se o intruso conseguir identificar os sinais será necessário retirar as amostras falsas do sinal 1 descobrindo as posições que ocupam e, então, o sinal voltará a possuir a taxa de transmissão e largura de banda originais. As posições que as amostras falsas ocupam estão na chave criptográfica. Sem essa chave demanda mais tempo e processamento para descobrir a onde estão as amostras falsas, tornando mais seguro a transmissão dos sinais.

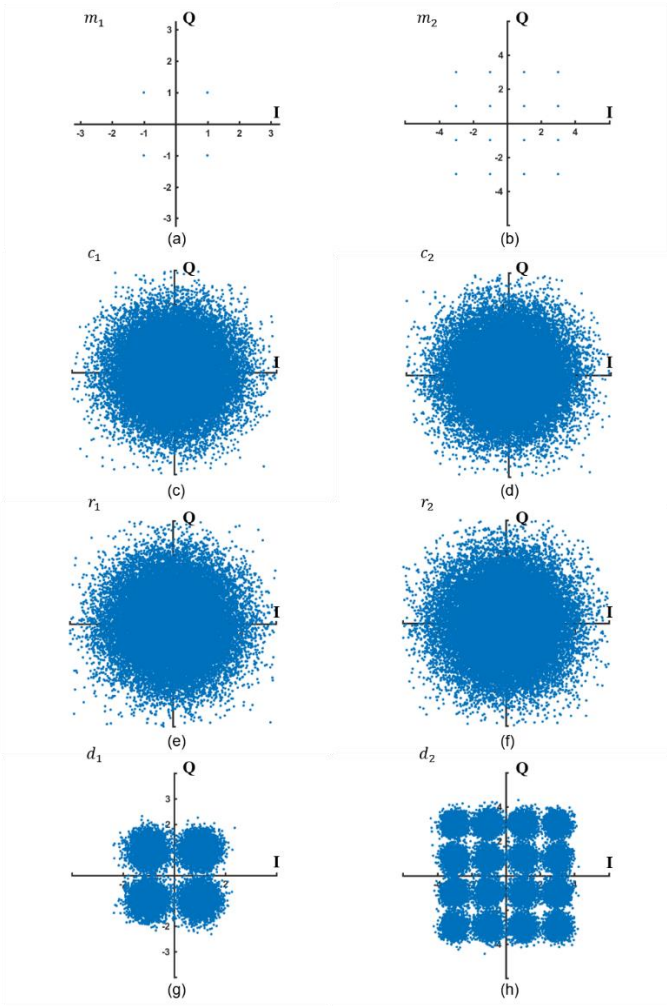

Figura 14 - Constelações obtidas com baixa SNR e com aplicação da segunda versão de taxas de transmissão distintas para o (a) primeiro sinal de entrada, (b) segundo sinal de entrada, (c) primeiro sinal criptografado, (d) segundo sinal criptografado, (e) primeiro sinal criptografado com ruído, (f) segundo sinal criptografado e com adição de ruído, (g) primeiro sinal descriptografado e recuperado e, (h) segundo sinal descriptografado e recuperado. Fonte: Autoria própria.

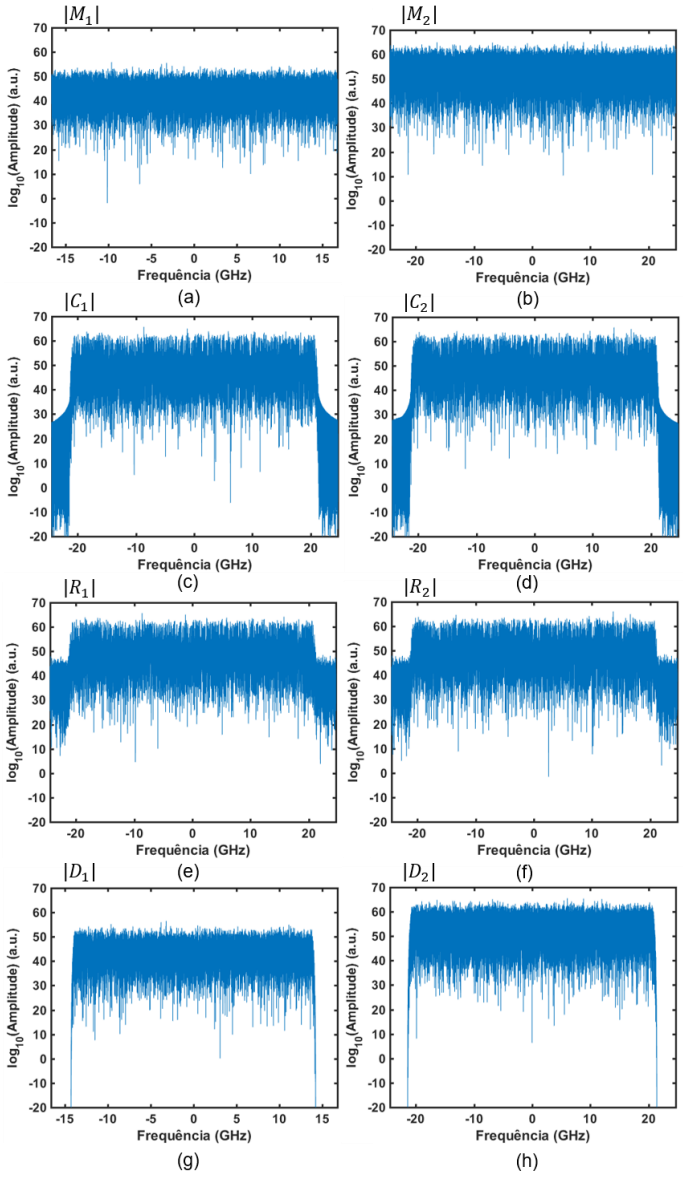

Figura 15 - Espectros de amplitude com baixa SNR e com aplicação da segunda versão de taxas de transmissão distintas para o (a) primeiro sinal de entrado, (b) segundo sinal de entrada, (c) primeiro sinal criptografado, (d) segundo sinal criptografado, (e) primeiro sinal criptografado e com ruído, (f) segundo sinal criptografado e com adição de ruído, (g) primeiro sinal descriptografado e recuperado e, (h) segundo sinal descriptografado e recuperado. Fonte: Autoria própria.

3.2. Análise da BER x SNR

Nessa Seção será discutido a partir dos valores da BER e da SNR se houve ou não penalidades aos sinais transmitidos e recuperados utilizando a técnica de criptografia SPE-SS-DSP com DK, aplicação de taxas de transmissão e sinalizações diferentes. Na Subseção 3.2.1 são discutidos os resultados da BER e da SNR com aplicação da primeira

versão de taxas de transmissão distintas. Na subseção 3.2.2 são discutidos os resultados da BER e da SNR com aplicação da segunda versão de taxas de transmissão distintas. O número de sinais gerados, transmitidos e recuperados foi de 2.

Na Figura 16 e Figura 18 são apresentados os resultados sem DK e com sinalizações iguais. O primeiro sinal e o segundo sinal estão modulados em 16-QAM em banda base. Os significados das siglas utilizadas nessas duas figuras e a ordem de obtenção das curvas durante as simulações são descritas a seguir:

1ª e 2ª Curva - Sinal Sem Criptografia: SSC;

3ª e 4ª Curva - Sinal Embaralhado/Desembaralhado e Codificado/Decodificado em Fase: SED-CDF;

5ª e 6ª Curva - Sinal Embaralhado/Desembaralhado e Codificado/Decodificado em Fase com Taxa de Transmissão Distinta: SED-CDF-TTD;

7ª e 8ª Curva - Sinal Embaralhado e Criptografado em Fase: SE-CF;

9ª e 10ª Curva - Sinal Embaralhado e Criptografado em Fase com Taxa de Transmissão Distinta: SE-CF-TTD.

Os resultados com DK e sinalizações diferentes são apresentados na Figura 17 e Figura *19*. O primeiro sinal está modulado em QPSK em banda base e o segundo sinal está modulado em 16-QAM em banda base. As siglas utilizadas nessas duas figuras e a ordem de obtenção das curvas durante as simulações são descritas a seguir:

1ª e 2ª Curva - Sinal Embaralhado/Desembaralhado, Codificado/Decodificado em Fase com Taxa de Transmissão Distinta e Modulação Distinta: SED-CDF-TTD-MD;

3ª e 4ª Curva - Sinal Embaralhado/Desembaralhado, Codificado/Decodificado em Fase com Taxa de Transmissão Distinta, Modulação Distinta e Chave Dinâmica: SED--CDF-TTD-MD-CD ;

4ª e 5ª Curva - Sinal Embaralhado, Codificado em Fase com Taxa de Transmissão Distinta e Modulação Distinta: SE-CF-TTD-MD;

6ª e 7ª Curva - Sinal Embaralhado, Codificado em Fase com Taxa de Transmissão Distinta, Modulação Distinta e Chave Dinâmica: SE-CF-TTD-MD-CD

3.2.1. BER x SNR com aplicação da primeira versão de taxas de transmissão distintas

Na Figura 16 são mostrados os sinais gerados sem criptografia em comparação com as técnicas de criptografia SS-DSP, SPE-SS-DSP e SPE-SS-DSP com aplicação da primeira versão de taxas de transmissão distintas. O sinais SED-CDF-TTD alcançam o limite da FEC para um valor de SNR igual a 18,56 dB. Os sinais criptografados apresentaram uma BER alta próxima de 0,5, dificultando a recuperação dos sinais transmitidos pelo canal para caso haja um intruso. As técnicas de criptografias em conjunto com aplicação da primeira versão de taxas de transmissão distintas não geraram penalidades aos sinais descriptografados e recuperados, pois apresentaram valores de BER e SNR muito próximos dos sinais sem criptografia transmitidos e recuperados.

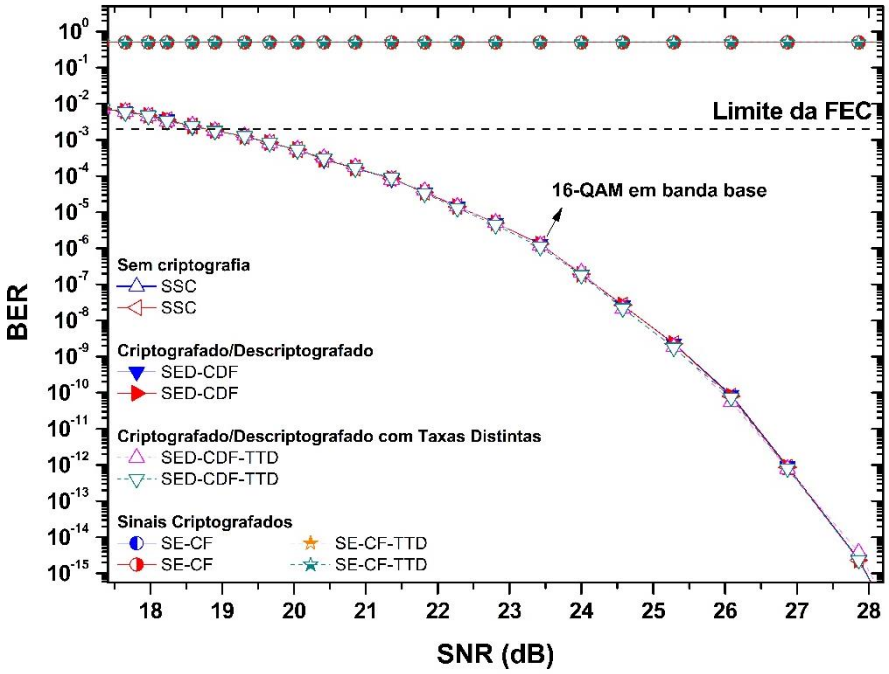

Figura 16 - Gráfico dos valores da BER e SNR para dois sinais transmitidos e recuperados em banda base com e sem técnicas de criptografias e com aplicação da primeira versão de taxas de transmissão distintas. Fonte: Autoria própria.

Na Figura 17 foi avaliado, em continuação da Figura 16, a qualidade dos sinais já criptografados e descriptografados, SED-CDF-TTD, com DK e sinalizações diferentes. O primeiro sinal QPSK considerando as curvas SED-CDF-TTD e SED-CDF-TTD-CD apresentou um valor de SNR próximo ao limite da FEC igual a 11,96 dB. Enquanto que o segundo sinal 16-QAM considerando as curvas SED-CDF-TTD e SED-CDF-TTD-CD apresentou a SNR próximo ao limite da FEC igual a 18,61 dB. Os sinais criptografados,

novamente apresentaram uma BER alta próxima de 0,5, dificultando a recuperação dos sinais transmitidos pelo canal para um intruso. As técnicas de criptografias com aplicação da primeira versão de taxas de transmissão distintas com sinalizações diferentes e chave dinâmica não geraram penalidades aos sinais descriptografados e recuperados, pois apresentaram valores de BER e SNR muito próximos dos sinais sem criptografias transmitidos e recuperados. Os valores de BER e de SNR são muito próximos dos resultados obtidos em (SANTOS, 2020).

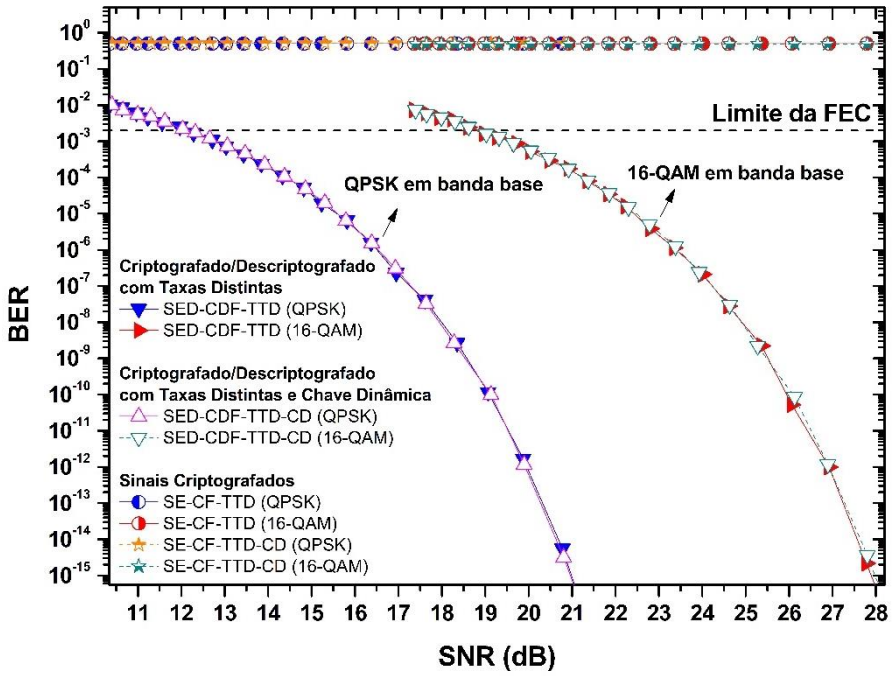

Figura 17 - Gráfico dos valores da BER e SNR para dois sinais transmitidos e recuperados em banda base com técnicas de criptografias, aplicação da primeira técnica de taxas de transmissão distintas, sinalizações diferentes e com chave dinâmica. Fonte: Autoria própria.

3.2.2. BER x SNR com aplicação da segunda versão de taxas de transmissão distintas

Os valores obtidos de BER e SNR do gráfico da Figura 18 e da Figura 19 foram muito semelhantes aos da Figura 16 e Figura 17 respectivamente. Na Figura 18 as curvas SED-CDF-TTD alcançaram o limite da FEC para um valor de SNR igual a 18,66 dB. O valor da SNR no limite da FEC é próximo do valor da SNR da primeira versão de taxas de transmissão distintas, possuindo uma diferença baixa de 0,10 dB.

As curvas SED-CDF-TTD e SED-CDF-TTD-CD do primeiro sinal QPSK na Figura *19* alcançaram o limite da FEC para um valor de SNR igual a 11,95 dB. O valor

da SNR alcançado no limite da FEC para o primeiro sinal é próximo em comparação com a primeira técnica de taxas de transmissão distintas, possuindo uma diferença muito baixa de 0,01 dB. Enquanto as curvas SED-CDF-TTD e SED-CDF-TTD-CD do segundo sinal 16-QAM alcançaram o limite da FEC para um valor de SNR igual a 18,59 dB. O valor da SNR no limite da FEC para o segundo sinal é próximo do valor da SNR da primeira versão de taxas de transmissão distintas, possuindo uma diferença baixa de 0,02 dB.

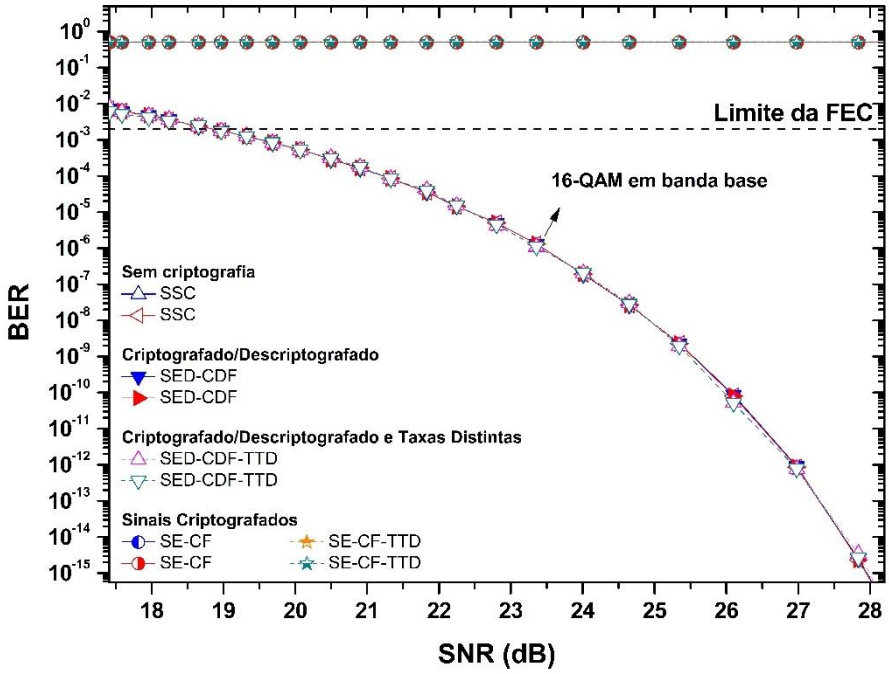

Figura 18 - Gráfico dos valores da BER e SNR para dois sinais transmitidos e recuperados em banda base com e sem técnicas de criptografias e com aplicação da segunda versão de taxas de transmissão distintas. Fonte: Autoria própria.

Na Figura 18 e Figura 19 é mostrado que os sinais criptografados com DK e a aplicação da segunda versão de taxas de transmissão distintas e sinalizações diferentes (curvas SED-CDF-TTD-CD) não resultaram em penalidades significativas aos sinais transmitidos e recuperados. As curvas SE-CF-TTD e SE-CF-TTD-CD do sinal 16-QAM possui valores da BER próximos a 0,5 e as curvas SE-CF-TTD e SE-CF-TTD-CD do sinal QPSK possui um valor de BER um pouco menor próximo de 0,40, dificultando a recuperação dos sinais transmitidos pelo canal para caso haja um intruso.

Os valores de BER e de SNR da Figura 17 e Figura 19 são muito próximos dos resultados obtidos em (SANTOS, 2020). Os resultados indicam serem corretos, pois foram obtidos em trabalhos anteriores em análises e desenvolvimento de outras técnicas de criptografias utilizando DSP.

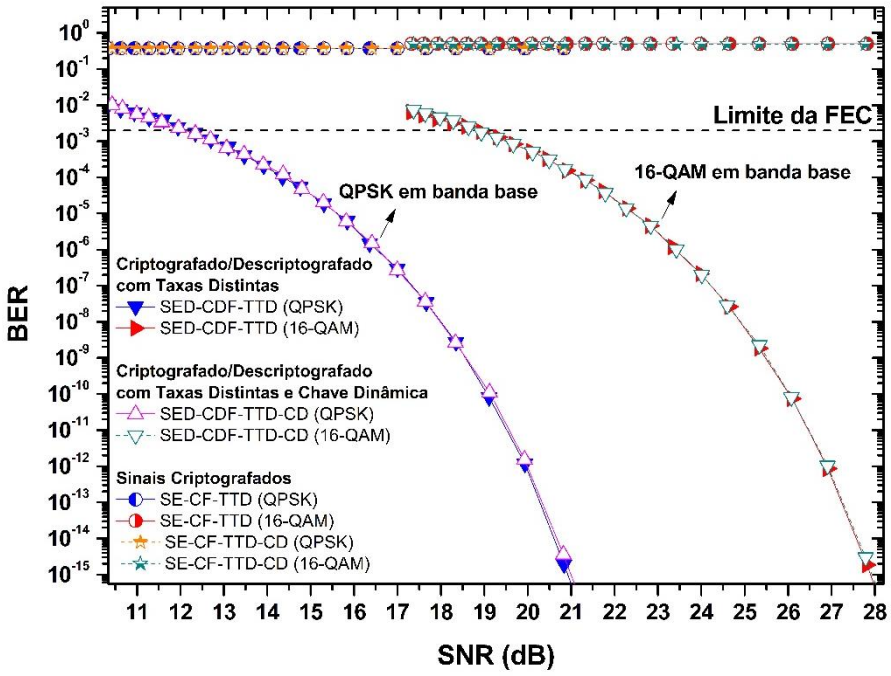

Figura 19 - Gráfico dos valores da BER e SNR para dois sinais transmitidos e recuperados em banda base com técnicas de criptografias, aplicação da segunda versão de taxas de transmissão distintas, sinalizações diferentes e chave dinâmica. Fonte: Autoria própria.

Na aplicação da segunda versão de taxas de transmissão distintas foi apresentado praticamente os mesmos valores da BER e da SNR comparadas com os valores da BER e da SNR da primeira versão de taxas de transmissão distintas. Além de tornar a transmissão dos sinais mais seguro, pois os dois sinais durante a transmissão possuem mesma largura de banda, mesma taxa de transmissão. Portanto, se para uma determinada comunicação é requerida mais confiabilidade, a segunda versão de taxas de transmissão distinta é mais viável. Enquanto que se para a comunicação é requerida o uso do espectro mais flexível, a primeira versão de taxas de transmissão distintas é mais viável.

4. CONCLUSÃO

As técnicas de criptografias abordadas neste trabalho foram de codificação de fase e embaralhamento espectral com implementação de chave dinâmica e aplicação a sinais com taxas de transmissão e sinalizações distintas. As novas melhorias de taxas de transmissão distintas em conjunto com sinalizações diferentes atendem ao requisito da EON de fazer o uso mais flexível do espectro. A EON é considerada como alternativa para suprir as altas taxas de transmissão de dados.

A diferença dos valores de SNR no limite da FEC entre as duas técnicas de transmissão de sinais com taxas distintas são muito baixas e iguais ou menores que 0,10 dB. Os gráficos da BER e SNR resultaram em curvas muito semelhantes entre os sinais de criptografados com melhorias e os sinais sem criptografias sem melhorias. Portanto, não houve penalidades significativas aos sinais descriptografados e recuperados ao utilizar as técnicas de criptografias desenvolvidas com chave dinâmica e melhorias desenvolvidas neste trabalho.

A segunda versão das taxas de transmissão distintas destaque-se em relação a primeira versão, pois o intruso, caso houver, não consegue identificar as diferenças da taxa de transmissão e largura de banda entre os sinais transmitidos, o que resulta em maior segurança. Enquanto que a primeira versão das taxas de transmissão distintas destaque-se em relação a segunda versão pela viabilidade de uso mais flexível do espectro durante a transmissão dos sinais.

As melhorias das técnicas de criptografias descritas e avaliadas neste trabalho atenderam o objetivo de manter a qualidade dos sinais sem causarem degradações e penalidades significativas aos sinais transmitidos e recuperados. As novas melhorias, portanto, mostraram uma boa eficiência e viabilidade de estudos e aplicações em redes ópticas e redes móveis.

5. REFERÊNCIAS

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 advanced modulation formats**. 16th International Conference on Transparent Optical Networks (ICTON). Graz, Austria: IEEE. 2014. Disponível em: 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, vol. 54. Disponível em: 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**, v. 32, n. 3, p. 154-157, Fevereiro. 2020. DOI: 10.1109/LPT.2019.2962837.

ABBADE, M. L. F. *et al.* **Signal Encryption Opportunities for Photonic Networks**. OSA Advanced Photonics Congress (AP) 2020 (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, 2020), paper NeTu1B.2. [S.l.]: [s.n.]. 2020. Disponível em: https://opg.optica.org/abstract.cfm?uri=Networks-2020-NeTu1B.2.

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

BIRYUKOV, A.; SHAMIR, A.; WAGNER, D. **Real Time Cryptanalysis of A5/1 on a PC**. Heidelberg: Springer, v. 1987, 2001. In: Goos G., Hartmanis J., van Leeuwen J., Schneier B. (eds) *Fast Software Encryption*. FSE 2000. Disponível em: https://doi.org/10.1007/3-540-44706-7_1.

BOBADILHA, 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.

CAMPBELL, D. **Revealed: GCHQ's beyond top secret Middle Eastern Internet spy base**, 3 Junho 2014. Disponivel em: https://www.theregister.com/2014/06/03/revealed_beyond_top_secret_british_intelligence_middleeast_Internet_spy_base/?page=1. Acesso em: 10 de Dezembro 2021.

CISCO. **Internet de Todas as Coisas no Setor Público**. Cisco e/ou suas afiliadas. [S.l.], p. 8. 2014.

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

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

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).

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.

DIFFIE, W.; HELLMAN, M. E. **New directions in cryptography**. **IEEE Trans. Inf. Theory**, v. 22, p. 644-654, Novembro. 1976.

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

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.

FIPS, N. **Announcing the Advanced Encryption Standard (AES)**. **National Institute of Standards and Technology**. [S.l.], p. 1-47. 2001. Disponível em: https://csrc.nist.gov/publications/detail/fips/197/final.

FURDEK, M.; SKORIN-KAPOV, N. **Physical-layer attacks in transparent optical networks**. **In:** FURDEK, M.; SKORIN-KAPOV, N. **Optical Communications Systems**. Rijeka: [s.n.], v. 3, 2012. Cap. 5, p. 123-146. ISBN 123-146.

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

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 de Dezembro 2021.

ITU. **Internet uptake has accelerated during the pandemic**. **Internet Telecommunications Union**, 2021. Disponivel em: https://www.itu.int/itu-d/reports/statistics/2021/11/15/Internet-use/. Acesso em: 20 de Novembro 2021.

ITU DEVELOPMENT SECTOR. **Measuring digital development Facts and figures 2021**. Internet Telecommunications Union. Geneva Switzerland, p. 23. 2021.

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

KEISER, G. **Comunicações por Fibras Ópticas**. Porto Alegre: AMGH: [s.n.], 2014. 1-696 p.

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

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, SK., Cai, WQ., Liu, WY. *et al.* **Satellite-to-ground quantum key distribution**. Publicado 9 de Agosto de 2017, *Nature* **549,** 43–47 (2017). https://doi.org/10.1038/nature23655

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

MOONEY, J. **Russian agents pluge to new ocean depths in Ireland to crack transatlantic cables, 16 Fevereiro 2020**. Disponivel em: https://www.thetimes.co.uk/article/russian-agents-plunge-to-new-ocean-depths-in-ireland-to-crack-transatlantic-cables-fnqsmgncz. Acesso em: 10 Dezembro 2021. Acesso em: 5 de Novembro de 2021.

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.

PALAIS, J. C. **Third Generation Transport Systems**. New Jersey: Prentice Hall: [s.n.], 2002. 1-352 p.

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

RIVEST, R. L.; SHAMIR, A.; ADLEMAN, L. A method for obtaining signatures and public-key cryptosystems, Commum, ACM, v. 21, p. 120-126, Fevereiro. 1978.

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.

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

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. *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.

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. Disponivel em: 10.1109/ICIT.2002.1189353.

TELEGEOGRAFY. **Submarine Cable Map**. 2021 Disponivel em: https://www.submarinecablemap.com/. Acesso em: 10 Dezembro 2021.

TychopouloS, A.; Koufopaulou, O.; Tomkos, I. **FEC in optical communications - A tutorial overview on the evolution of architectures and the future prospects of outband and inband FEC for optical communications**. Circuits and Devices Magazine, *IEEE*, v.22, p. 79 - 86, 12 2006.

WAGNER, D.; SCHNEIER, B.; KELSEY, J. **New directions in cryptography**. **IEEE Trans. Inf. Theory**, v. 22, p. 644-654, Novembro. 1976.

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

YENER, A.; ULUKUS, S. **Wireless Physical-Layer Security: Lessons Learned From Information Theory**. **Proceedings of the IEEE**, Outubro. 2015. DOI: 10.1109/JPROC.2015.2459592.

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.