UNIVERSIDADE ESTADUAL PAULISTA
"JÚLIO DE MESQUITA FILHO"
CAMPUS DE SÃO JOÃO DA BOA VISTA

JOÃO GABRIEL TEIXEIRA

Verificação Experimental do Desempenho de Técnicas de Criptografia de Sinais

São João da Boa Vista
2024

João Gabriel Teixeira

Verificação Experimental do Desempenho de Técnicas de Criptografia de Sinais

Trabalho de Graduação apresentado ao Conselho de Curso de Graduação em Engenharia Eletrônica e de Telecomunicações do Campus de São João da Boa Vista, Universidade Estatual Paulista, como parte dos requisitos para obtenção do diploma de Graduação em Engenharia Eletrônica e de Telecomunicações .

Orientador: Profº Dr. Marcelo Luís Francisco Abbade

São João da Boa Vista
2024

T266v

Teixeira, João Gabriel
Verificação experimental do desempenho de técnicas de criptografia de sinais / João Gabriel Teixeira. -- São João da Boa Vista, 2024
43 p. : tabs., fotos

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

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

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

DADOS CURRICULARES

JOÃO GABRIEL TEIXEIRA

NASCIMENTO 13/05/1998 - Casa Branca / SP

FILIAÇÃO Rinaldo Donizeti Teixeira
Maria Aparecida de Paula Teixeira

2016 / 2024 Bacharel em Engenharia Eletrônica e de Telecomunicações
Universidade Estadual Paulista "Júlio de Mesquita Filho"

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

TRABALHO DE CONCLUSÃO DE CURSO

VERIFICAÇÃO EXPERIMENTAL DO DESEMPENHO DE TÉCNICAS DE CRIPTOGRAFIA DE SINAIS

Aluno: João Gabriel Teixeira
Orientador: Prof. Dr. Marcelo Luís Francisco Abbade

Banca Examinadora:

- Marcelo Luís Francisco Abbade (Orientador)
- Ivan Aritz Aldaya Garde (Examinador)
- Wilian Miranda dos Santos (Examinador)

A ata da defesa com as respectivas assinaturas dos membros encontra-se no prontuário do aluno (Processo nº 199/2023)

São João da Boa Vista, 28 de junho de 2024

AGRADECIMENTOS

Em primeiro lugar, agradeço a Deus por me dar forças para seguir sempre em frente.

Gostaria de expressar minha sincera gratidão aos meus pais, Rinaldo e Maria Aparecida, que não mediram esforços para me manter financeiramente, sempre me apoiando em decisões e escolhas nas quais fiz para realizar meus sonhos.

Aos meus irmãos, Rafael e Vanessa por todo apoio emocional, estando sempre ao meu lado em todo o período de graduação.

Aos meus colegas de curso, Grazielle Cossa, Lucas Cardoso, Lucas Viana, Mateus Lopes, Nicole Lopes, Nawar Darweesh, Otávio Mendonça, Thallysson Souza e bibliotecário João Cardoso. Amigos muito especiais, que mais estiveram próximos a mim durante todo o ciclo de graduação, sempre adquirindo novas conquistas juntos.

A todos os docentes, pela dedicação e por nos preparar para os desafios profissionais que enfrentaremos. Em especial, agradeço aos meus orientador Marcelo Luís Francisco Abbade e Professor Ivan Aritz Aldaya Garde, por toda paciência e dedicação para com minha pessoa.

Por fim, a todos que estiveram comigo em todo este percurso, gerando em minha memória, momentos inesquecíveis.

Este trabalho contou com o apoio da(s) seguinte(s) entidade(s):
UNESP - Universidade Estadual Paulista "Júlio de Mesquita Filho"

“Quando vocês acham que as pessoas morrem? Quando elas levam um tiro de pistola bem no coração? Não. Quando são vencidas por uma doença incurável? Não! Quando bebem uma sopa de cogumelo venenoso? Não! Elas morrem... quando são esquecidas.“

(Hiluluk - Eiichiro Oda)

RESUMO

O objetivo deste trabalho foi avaliar experimentalmente uma técnica de criptografia de sinais que combina i) codificação espectral de fase e ii) embaralhamento intracanal. Essas técnicas foram aplicadas a um sinal em banda-base de entrada, que após receber este processo de codificação, resulta em um sinal em banda-base distorcido em acordo com uma chave criptográfica. Este sinal foi transmitido por um equipamento transceptor, em uma configuração back-to-back sem a adição de ruído. Um cabeçalho, chamado de piloto, foi adicionado ao sinal encriptado para permitir a escolha dos instantes de amostragem. A análise do sinal foi realizada offline. A recuperação do sinal foi bem realizada para cerca de 92% dos bits. Trabalhos futuros devem aprimorar o código de recepção usado para aumentar esta taxa de acerto para valores iguais ou, pelo menos, muito próximos a 100%.

PALAVRAS-CHAVE: Criptografia de Sinais. Segurança. Codificação Espectral de Fase. Embaralhamento Espectral.

ABSTRACT

The objective of this study was to experimentally evaluate a signal encryption technique that combines i) spectral phase encoding and ii) intracanal scrambling. These techniques were applied to a baseband input signal, which, after undergoing this encoding process, resulted in a distorted baseband signal according to a cryptographic key. This signal was transmitted using a transceiver device in a back-to-back configuration without added noise. A header, referred to as a pilot, was added to the encrypted signal to enable the selection of sampling instants. Signal analysis was conducted offline. The signal was successfully recovered for approximately 92% of the bits. Future work should focus on improving the reception code to increase this success rate to values equal to or at least very close to 100%.

KEYWORDS: Signal Encryption. Security. Spectral Phase Encoding. Scrambling Cryptography.

LISTA DE ILUSTRAÇÕES

LISTA DE ABREVIATURAS E SIGLAS

AES	Advanced Encryption Standard - Padrão de Criptografia Avançado
BER	Bit Error Rate - Razão de Erro de Bits
CPU	Central Processing Unit - Unidade Central de Processamento
CSV	Comma-separated Values - Arquivo Separado Por Vírgula
DC	Direct Current - Corrente Contínua
FFT	Fast Fourier Transform - Transformada Rápida de Fourier
HTTP	HyperText Transfer Protocol - Protocolo de Transferência de Hipertexto
IFFT	Inverse Fast Fourier Transform - Transformada Rápida de Fourier Inversa
IP	Internet Protocol - Protocolo de Internet
IPSec	Internet Protocol Security - Protocolo de Segurança IP
ISI	Intersymbol Interference - Interferência Intersimbólica
LAN	Local Area Network - Rede Local
NRZ	Non Return to Zero - Não Retorno a Zero
PRBS	Pseudo Random Bit Sequence - Sequência Pseudoaleatória de Bits
PCS	Physical Coding Sublayer - Subcamada de Codificação Física
PMD	Physical Medium Dependent Sublayer - Subcamada Dependente do Meio Físico
RCF	Raised Cosine Filter - Filtro Cosseno Levantado
RF	Radio Frequency - Radiofrequência

SPE	Spectral Phase Encoding - Codificação Espectral de Fase
SS	Spectral Shuffled - Embaralhamento Espectral
SSL	Secure Sockets Layer - Camada de Soquetes Seguros
TCP	Transmission Control Protocol - Protocolo de Controle de Transmissão
TCC	Trabalho de Conclusão de Curso
TLS	Transport Layer Security - Segurança da Camada de Transporte
USB	Universal Serial Bus - Porta Serial Universal
WPA3	Wi-Fi Protected Access 3 - Acesso Protegido por Wi-Fi 3
WWW	World Wide Web - Rede Global de Computadores

LISTA DE SÍMBOLOS

$m(k)$	Cabeçalho no domínio temporal
$M(k)$	Cabeçalho no domínio espectral
$p(k)$	*Payload* no domínio temporal
$g(k)$	Sinal Gerado no domínio temporal
$e(k)$	Sinal Gerado e encriptado no domínio temporal
$u(k)$	Sinal de exemplo para embaralhamento
$u_e(k)$	Sinal de exemplo criptografado por embaralhamento
K_s	Chave de Embaralhamento
K_p	Chave de Fase
Sa	Amostras
r	Fator de Decaimento do Filtro Cosseno Levantado
B_l	Largura de Banda limitada do sinal pelo Filtro Cosseno Levantado
θ_i	Fase da i-ésima amostra
R_{SY}	Taxa de Transmissão de Simbolo

SUMÁRIO

1 INTRODUÇÃO

1.1 A IMPORTÂNCIA DA CRIPTOGRAFIA

A criptografia desempenha um papel essencial na sociedade contemporânea, sendo fundamental para garantir a segurança, privacidade e confidencialidade em todas as formas de comunicação. Ela permite que informações sensíveis sejam protegidas contra receptores ou ouvintes não autorizados, garantindo que apenas os destinatários legítimos possam acessar o conteúdo.

As primeiras formas de criptografia remontam às civilizações antigas, tornando-se um dos campos mais antigos de estudo técnico. Registros históricos indicam que práticas criptográficas datam de pelo menos 4000 anos atrás (COHEN, 1995). Um exemplo disso são os métodos de criptografia utilizados pelos gregos. Entre os gregos antigos, especificamente os espartanos, guerreiros do povo grego, foi utilizado o primeiro sistema de criptografia militar (ARAÚJO, 2018). Um método notável era o uso da *Scytale*, um dispositivo cilíndrico utilizado para criptografar mensagens ao enrolar uma tira de pergaminho em torno do cilindro. Essa ação alinhava o texto de forma legível apenas quando envolto corretamente, utilizando outro cilindro de mesmo diâmetro e espessura.

Na Idade Contemporânea, especificamente nos séculos XX e XXI, houve um aumento significativo na pesquisa e desenvolvimento de técnicas de criptografia, especialmente após a Primeira e a Segunda Guerras Mundiais. Até a Segunda Guerra, os métodos de criptografia eram baseados em letras. Por exemplo, os alemães possuíam uma máquina conhecida como "Enigma". Esse dispositivo era uma máquina eletromecânica de rotores, utilizada para cifrar e decifrar códigos de guerra. Ela foi inventada pelo engenheiro eletricista alemão Arthur Scherbius, que a patenteou como uma máquina de cifragem que usa rotores, em fevereiro de 1918 (ARAÚJO, 2018). Concomitante à Segunda Guerra, surgiu o primeiro computador, e a criptografia passou a ser baseada em algoritmos que operam sobre bits. Nesse contexto, o trabalho de Claude Shannon, divulgado em 1948 e intitulado "*A Communications Theory of Secrecy Systems*", tornou-se a base da criptografia computacional atual.

Com o advento da computação e da Internet, a criptografia tornou-se ainda mais essencial para a proteção das comunicações digitais e dos dados pessoais. A proliferação de transações financeiras online, comunicações por e-mail e armazenamento de

dados na nuvem trouxe novos desafios e ameaças, exigindo soluções criptográficas robustas para garantir a integridade e a confidencialidade das informações. Com isso, houve a criação de algoritmos, como o *Advanced Encryption Standard* (AES), que é um exemplo de uma das várias técnicas criptográficas de segurança de rede (TANENBAUM, 2002). O AES, por exemplo, é amplamente utilizado em diversas aplicações, desde a proteção de dados em dispositivos móveis até a segurança de transações bancárias. Este algoritmo de encriptação é baseado em uma cifra de bloco que, a partir de uma chave criptográfica, encripta blocos de 128 bits. O AES foi aceito como padrão pelo *National Institute of Standards and Technology* (Instituto Nacional de Padrões e Tecnologia) em 2001, órgão do Departamento de Comércio estadunidense responsável por aprovar padrões para o governo federal estadunidense (TANENBAUM, 2002).

A criptografia é indispensável na proteção das informações sensíveis na sociedade atual. Desde suas formas mais primitivas nas civilizações antigas até os algoritmos complexos da era digital, a criptografia continua a evoluir, adaptando-se às novas demandas e desafios impostos pelo avanço tecnológico. A continuidade da pesquisa e desenvolvimento em criptografia é crucial para manter a segurança e a privacidade em um mundo cada vez mais conectado e digital.

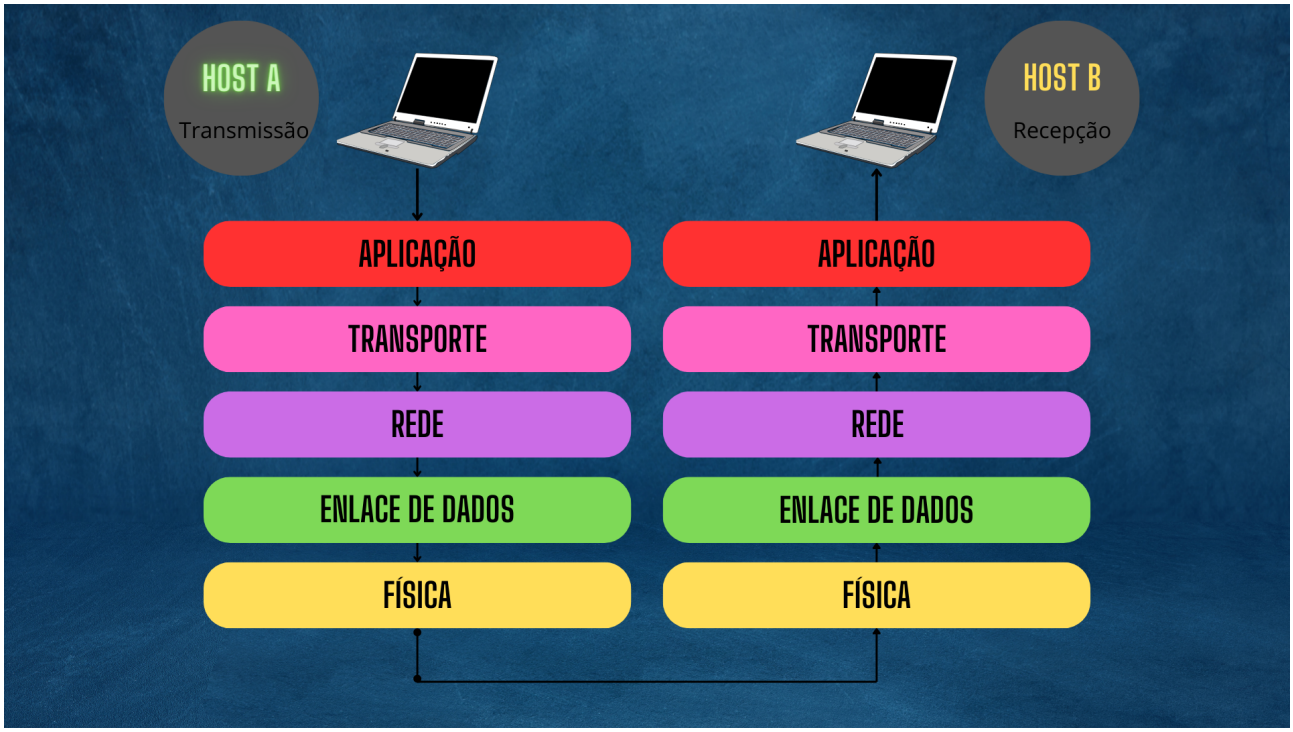
1.2 CRIPTOGRAFIA DE DADOS

A criptografia de dados é um campo especializado focado na proteção de informações digitais, ou seja, em bits, por meio de técnicas de codificação. Este domínio é crucial para a segurança da informação, que é baseada na tríade da segurança - confidencialidade, integridade e disponibilidade *(Confidentiality, Integrity and Availability*, CIA) dos dados em diversos contextos, incluindo transações financeiras, comunicações pessoais e empresariais, e armazenamento de dados local e em nuvem. A criptografia desempenha um papel crítico na segurança da informação, oferecendo uma defesa robusta contra acesso não autorizado e ataques maliciosos. A capacidade de proteger informações sensíveis é vital para manter a confiança nas operações digitais e para cumprir regulamentos de proteção de dados. Os princípios de confusão e difusão propostos por Claude Shannon estabelecem características mínimas de segurança para algoritmos de criptografia de dados (SHANNON, 1949). A confusão visa tornar a relação entre a chave de criptografia e o texto cifrado a mais complexa possível, dificultando a previsão do texto original a partir do texto cifrado. A difu-

são, por outro lado, assegura que pequenas mudanças no texto original resultem em grandes alterações no texto cifrado, ampliando a resistência a ataques estatísticos.

No contexto do tráfego de informações, a criptografia é frequentemente implementada nas camadas superiores da arquitetura de redes. Desde o momento em que uma mensagem é enviada pela rede até sua entrega ao destinatário, a criptografia assegura que os dados permaneçam inacessíveis a interceptores não autorizados. Consideramos então as camadas de aplicação, transporte, rede, enlace de dados e física de uma arquitetura de rede de cinco camadas, ilustrada na Figura 1.

Figura 1 – Arquitetura de Redes de 5 camadas.



Fonte: Autoria Própria.

Estas camadas são frequentemente responsáveis por implementar protocolos criptográficos que protegem os dados durante a transmissão. A seguir, apresenta-se algumas das características dessas camadas:

- Camada de Aplicação: A camada de aplicação abrange os protocolos essenciais para a comunicação entre os usuários e os sistemas, como o Protocolo de Transferência de Hipertexto *(HyperText Transfer Protocol*, HTTP), que serve como a fundação para a rede global de computadores *(World Wide Web*, WWW). Quando um navegador solicita uma página da web, ele envia uma requisição (ou simplesmente o nome da página requisitada) ao servidor utilizando o protocolo

HTTP. Em resposta, o servidor envia de volta a página solicitada ao navegador (TANENBAUM, 2002). A interação entre o cliente *(browser)* e o servidor *(site)* é fundamental para essas aplicações, caracterizando uma comunicação cliente-servidor, na qual ambas as partes trocam informações de maneira direta.

- Camada de Transporte: Na camada de transporte, os dados podem ser protegidos por protocolos de segurança, como o protocolo Camada de Soquetes Seguros (*Secure Sockets Layer*, SSL) e seu sucessor, o protocolo Segurança da camada de transporte (*Transport Layer Security*, TSL), que garantem a segurança das informações antes de serem transmitidos pelo Protocolo de Controle de Transmissão *(Transmission Control Protocol*, TCP), um protocolo orientado à conexão, responsável por resolver problemas como pacotes perdidos ou corrompidos devido a erros de transmissão (FERNÁNDEZ, 2019). Esses protocolos asseguram a confidencialidade e a integridade dos dados, enquanto o TCP garante a transmissão ordenada e sem erros dos pacotes.

- Camada de Rede: A camada de rede é responsável pelo encaminhamento de pacotes desde sua origem até o destino final, ou seja, atua na comunicação entre as máquinas *(hosts)* de uma rede, passando por todos os dispositivos intermediários (FERNÁNDEZ, 2019). Portanto, ela realiza a troca de pacotes entre os computadores conectados via Internet, determinando o melhor caminho e garantindo a segurança e integridade dos dados transmitidos, utilizando, por exemplo, o protocolo de Segurança IP *(IP Security*, IPSec), que oferece criptografia e proteção contra ataques de reprodução, usando chave simétrica e permitindo a escolha de algoritmos e serviços conforme a necessidade dos usuários (TANENBAUM, 2002).

- Camada de Enlace de Dados: Na camada de enlace de dados, a criptografia é empregada para assegurar a integridade e a confidencialidade dos quadros durante sua transmissão na rede local. O protocolo Acesso Protegido por Wi-Fi 3 *(Wi-Fi Protected Access 3*, WPA3) é um exemplo de criptografia utilizada nessa camada, com o objetivo de proteger redes sem fio contra acessos não autorizados. O WPA3 opera em dois modos: WPA3-Pessoal e WPA3-Enterprise, sendo responsável pela proteção de quadros de gerenciamento e pela mitigação de ataques de desautenticação, nos quais agentes maliciosos

tentam forçar os usuários a desconectarem-se do ponto de acesso (HALBOUNI; ONG; LEOW, 2017).

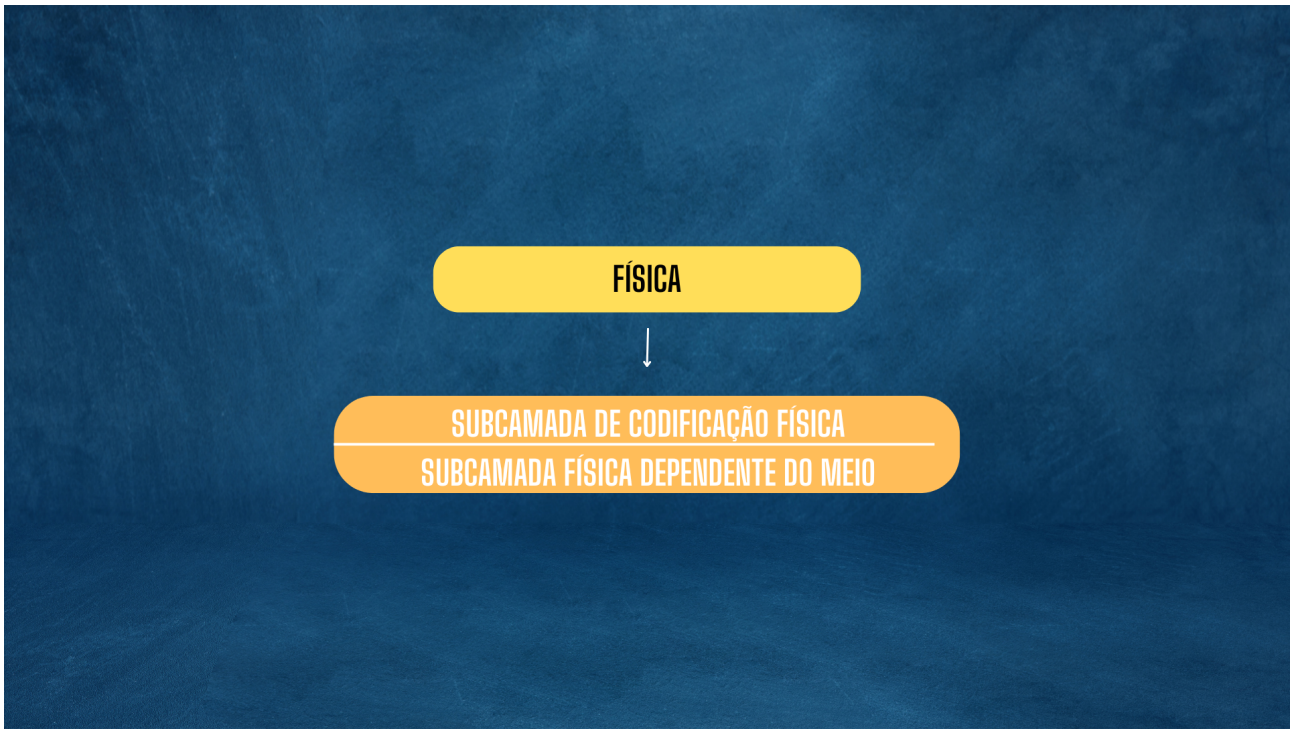
- Camada Física:

  A camada física converte bits em sinais físicos. Apesar de existirem propostas de pesquisa para criptografar estes sinais (SANTOS, 2020), (NOGUEIRA, 2022), (ABBADE et al., 2019), (ZHAO; JIANG; LIU; ZHANG; QIU, 2021), (LI; MCLERNON; LEI; GHOGHO; ZAIDI; HUI, 2019), este tipo de criptografia não é realizado em sistemas comerciais. Isto gera uma brecha de segurança na camada física.

1.3 CRIPTOGRAFIA DE SINAIS

Na última subseção, foram apresentadas informações sobre a criptografia de dados aplicada ao modelo de arquitetura de redes de cinco camadas, e foi mencionado que a criptografia de sinais não é utilizada comercialmente. Essa camada pode ser dividida em duas subcamadas, conforme ilustrado na Figura 2:

Figura 2 – Camada Física dividida em duas subcamadas.



Fonte: Autoria Própria.

A subcamada superior da camada física, denominada Subcamada de Codificação Física (*Physical Coding Sublayer*, PCS), tem funções como transformar bits em símbolos e, em seguida, transmitir essa informação para a subcamada inferior da camada física, chamada Subcamada Física Dependente do Meio (*Physical Medium Dependent Sublayer*, PMDS). A PCS é responsável pela codificação e decodificação dos dados transmitidos via a algum tipo de interface física (BARBIERI, 2005). A subcamada PMDS, converte os bits em sinais, e esses sinais não são criptografados durante a transmissão. Diante disto, torna-se crucial a adoção de criptografia de sinais, que difere da criptografia de dados utilizada nas camadas superiores da arquitetura de cinco camadas. Em cenários usuais, sabe-se que o proprietário das informações não é também o proprietário da rede pela qual essas informações trafegam, isso cria uma vulnerabilidade significativa, permitindo que agentes mal-intencionados instalem dispositivos de interceptação para redirecionar informações para destinos não autorizados.Enquanto a criptografia de dados emprega protocolos padronizados e amplamente aceitos, ainda há a necessidade de desenvolvimento de protocolos padronizados para criptografia de sinais. Espera-se que a criptografia de sinais seja compatível com os métodos de Confusão e Difusão de Shannon, assim como foi abordado pelo trabalho (SANTOS, 2020) no uso de Processamento Digital de Sinais *(*Digital Signal Processing, DSP). Implementar criptografia de sinais, envolve diversos desafios, incluindo a necessidade de desenvolver novos padrões e protocolos específicos para essa camada. Além disso, a criptografia de sinais deve ser eficiente o suficiente para não degradar a qualidade do serviço, mantendo a integridade e a confiabilidade da comunicação.

1.4 OBJETIVO DO TRABALHO

O objetivo deste trabalho é analisar técnicas de criptografia, como a Codificação Espectral de Fase *(Spectral Phase Encoding*, SPE) e o Embaralhamento Espectral *(Spectral Scrambling*, SS) de forma experimental, utilizando um transceptor e verificar se os resultados obtidos foram satisfatórios.

Vale ressaltar que essas técnicas foram previamente validadas por meio de simulações realizadas especificamente na dissertação de (SANTOS, 2020), intitulada "Criptografia na Camada Física Baseada em Codificação Espectral Implantada por Meio de DSP e Aplicada a Redes Ópticas". Este estudo investigou técnicas de criptografia de sinais, destacando-se entre elas SPE e SS.

No entanto, é importante notar que tais técnicas ainda não foram examinadas experimentalmente por nosso grupo de pesquisa. Portanto, há necessidade premente de verificar essas técnicas de forma experimental. Para isto, foi utilizado o equipamento *M9046A High-Power PXIe Chassis*, recém adquirido pela Faculdade de Engenharia de São João da Boa Vista (FESJ - UNESP). Esse equipamento trata-se de um transceptor, dispositivo modular que permite a transmissão de dados por meio de um pequeno enlace até seu receptor integrado. Este equipamento proporciona controle sobre tipos de modulação, frequência e diversas características dos canais, possibilitando a aproximação dos resultados às condições desejadas.

2 CONCEITOS, METODOLOGIA UTILIZADA E TÉCNICAS DE CRIPTOGRAFIA DE SINAIS

A criptografia de sinais é essencial para garantir um grau maior de confidencialidade da informação. Neste capítulo, serão detalhadas a metodologia das técnicas de criptografia empregados neste estudo e de como foram feitas as verificações experimentais por meio do equipamento transceptor. A seção 2.1 abordará a forma pela qual foram convencionados os identificadores dos sinais a serem utilizados e o esquema seguido para obtenção dos resultados. A seção 2.2 descreverá o transceptor utilizado nos experimentos. A seção 2.3 apresentará a metodologia usada para gerar os sinais utilizados nos experimentos. E por fim, a seção 2.4 descreverá as técnicas de criptografia aplicadas aos sinais.

2.1 CONVENÇÕES E ESQUEMAS DE EXECUÇÃO

Convencionou-se que os sinais no domínio temporal serão denominados por letras minúsculas, enquanto os sinais no domínio espectral serão denominados por letras maiúsculas. Para a representação dos sinais contendo a carga útil, utilizamos a letra "p"ou "P", e para o cabeçalho, a letra "m"ou "M". Junto às letras, será anexado um número inteiro natural que representa qual sinal está sendo tratado. Por exemplo, $p[k]$ é o *payload* no domínio temporal. Como o presente trabalho faz uso de sinais digitais e discretizados, a letra "k"será anexada para indicar as componentes amostrais. O Quadro 1 apresenta essas condições:

Quadro 1 – Sinais Utilizados

Sinais	Domínio	Representação
Cabeçalho	Temporal	$h[k]$
Cabeçalho	Espectral	$H[k]$
Payload	Temporal	$p[k]$
Payload	Espectral	$P[k]$

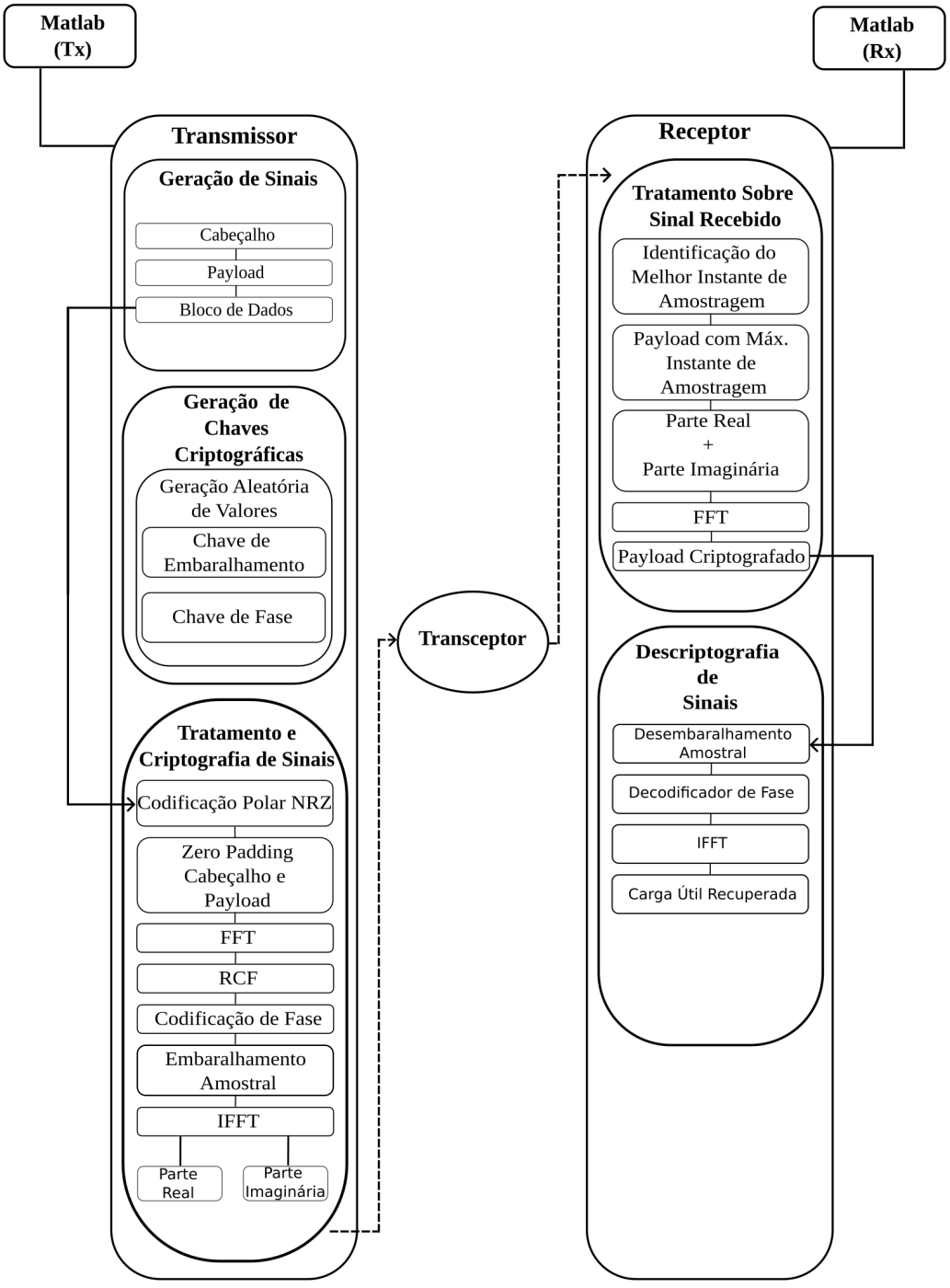
fonte: Autoria Própria.

O método aplicado para obter os respectivos sinais no domínio da frequência, foi utilizar a transformada rápida de Fourier (*Fast Fourier Transform*, FFT) dos sinais $h[k]$, $p[k]$ (LATHI;DING, 2012).

No diagrama da Figura 3, temos a organização esquemática do código gerador de arquivo de sinal amostrado e de criptografia, sua interação com o equipamento

transceptor e, por fim, o código de tratamento das informações recebidas no receptor, incluindo a descriptografia do sinal e sua recuperação.

Figura 3 – Diagrama Modular dos Processos Realizados para a Geração, Codificação, Transmissão, Recepção e Tratamento dos Sinais.



Fonte: Autoria Própria.

Existe um *software* intitulado de KryptoSJ e foi desenvolvido por um grupo de

estudos da UNESP-SJBV. Nele são utilizadas técnicas de criptografia como Criptografia de codificação espectral de fase e embaralhamento intra-canal por processamento digital de sinais (DSP-SPE-Scr) (SANTOS, 2020) e Embaralhamento espectral e codificação espectral de fase e de atraso baseado em DSP (SPDE-SS-DSP) (NOGUEIRA, 2022). Com os resultados obtidos por meio das simulações nesses trabalhos, há o desejo de realizar verificações em equipamentos reais, visando uma futura aplicação comercial. O algoritmo de criptografia utilizado nos códigos do *software* foi desenvolvido recentemente pelo Prof. Dr. Marcelo Abbade, e é similar à outros algorítimos desenvolvidas no KryptoSJ. Neste trabalho, usou-se o código com as técnicas de criptografias de fase, embaralhamento e desembaralhamento em conjunto com transmissão de sinais de impulsos em banda-base. Os módulos que se referem a parte de Geração, Codificação e Tratamento dos Sinais, foram realizados no *Software* Matlab®.

2.2 TRANSCEPTOR

Para realizarmos a verificação experimental, utilizamos um transceptor adquirido pela UNESP para estudos de comunicações via enlaces de guias de onda de RF. A subseção 2.2.1 apresentará as características sobre o Módulo de Processamento do Transceptor. A subseção 2.2.2 descreverá os Módulos de Transmissão e Recepção, respectivamente e suas operações.

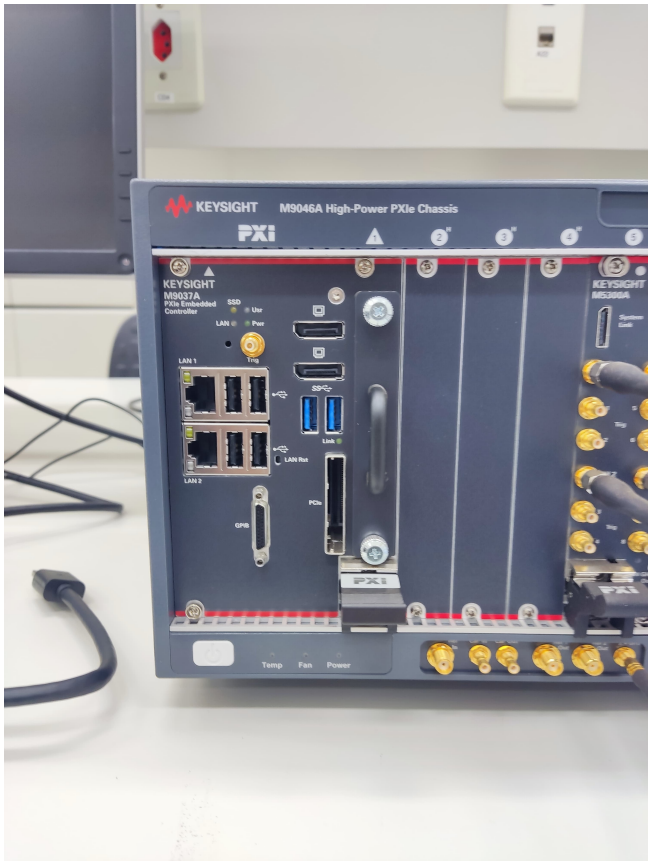
2.2.1 Modulo de Processamento do Transceptor

A Figura 4 apresenta o módulo de processamento do equipamento. Este módulo é uma Unidade Central de Processamento (*Central Processing Unit, CPU*), baseada no sistema operacional *Windows* 10, que permite avaliar os experimentos realizados pelos módulos de transmissão e recepção.

As suas principais características são:

- Processador Intel i7-4700EQ 2,4 GHz
- Processador multinúcleo Quad-Core
- 16 GB de memória RAM
- Conexão do painel frontal com USB 2.0 (4), USB 3.0 (2), LAN (10/100/1000) (2), DisplayPort (2), GPIB e gatilho SMB

Figura 4 – Módulo de Processamento do Transceptor.



fonte: Autoria Própria.

Por meio das conexões USB no painel frontal, podemos realizar a transferência de arquivos. Esses arquivos serão gerados pelo *software* MATLAB®. Para o transceptor gerar esses sinais, é necessário informar quais são as amostras que representam o sinal, o que é feito por meio de um arquivo .CSV. No caso do experimento realizado, esse arquivo foi gerado a partir do código de encriptação dos sinais.

2.2.2 Módulos de Transmissão e Recepção

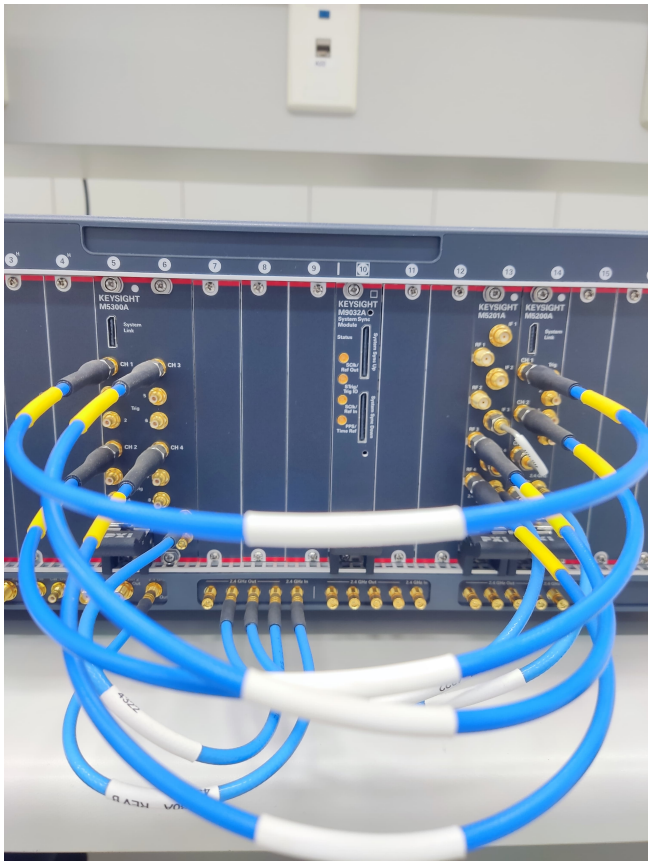
A Figura 5 apresenta os módulos de transmissão e recepção do equipamento.

O M5300A (Módulo ocupando os *slots* 5 e 6) é o transmissor, ele suporta 4 canais de RF, que são geradores de formas de onda arbitrárias de alta velocidade com entrada e saída de *clock* e oito *triggers*. Este módulo opera na faixa de DC até frequências de portadoras de 16 GHz. A largura de banda do sinal admitido é de até 2 GHz.

As suas principais características são:

- Geração de Formas de Onda Analógicas na faixa DC à 16 GHz
- Transmissão de Sinais em Banda Base

Figura 5 – Transceptor Utilizado nos Experimentos



Fonte: Autoria Própria.

- Transmissão de Sinais com Modulação Digital
- Taxa de Amostragem de 2,4 GSa/s
- Memória de Forma de Onda para cada canal, com até 1 GSa

O M5200A (Módulo ocupando o slot 14) é o receptor, assim como o transmissor, ele também suporta 4 canais de RF e é um digitalizador analógico para digital de alta velocidade e desempenho.

As suas principais características são:

- Quatro canais de 2 GHz
- Recepção de Sinais em Banda Base
- Recepção de Sinais com Modulação Digital
- Taxa de Amostragem de 4,8 GSa/s

2.3 GERAÇÃO DE SINAIS

Esta seção aborda a metodologia utilizada para gerar um arquivo que conterá a informação a ser transmitida de forma criptografada pelo transceptor utilizado para verificação experimental.

A representação da nossa informação será de uma sequência de bits, que se inicia com um cabeçalho e que será concatenado a um *payload* contendo a carga útil do sinal. O cabeçalho é adicionado para que possamos identificar o melhor instante de amostragem, e o método utilizado será explicado posteriormente. Quando criptografamos um sinal em banda-base e essa informação é enviada por um canal, quando entregue ao receptor, é necessário que identifiquemos qual o melhor momento para iniciar sua amostragem. Para isso, basta adicionarmos um cabeçalho concatenado à carga útil a ser transmitida e que é denominado de piloto, destacando onde o cabeçalho finaliza e onde a informação criptografada inicia (CARDOSO, 2022). O cabeçalho foi composto por uma sequência de bits 1's e 0's alternados.

O *payload* do nosso sinal será dado utilizando uma sequência pseudoaleatória de bits *(Pseudo Random Bit Sequence*, PRBS), passará pelo processo de encriptação, e por fim será concatenado ao cabeçalho, gerando o nosso bloco de dados.

2.3.1 Codificação Polar

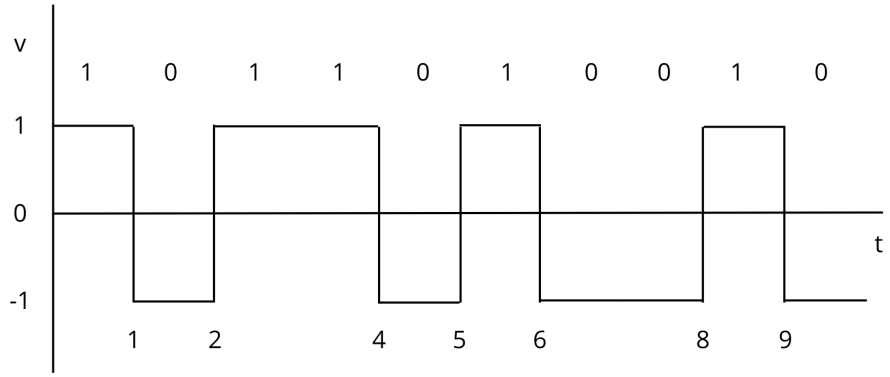
Os sinais são do tipo de códigos de linha, que são a transformação de uma sequência binária em sua representação elétrica. A princípio, temos uma sequência de bits que irão representar o nosso sinal a ser transmitido. Essa sequência de bits advém da concatenação entre cabeçalho e *payload*.

Para diminuir o risco de erro de bit, escolheu-se a representação da sequência de bits na forma de impulsos polares, utilizando o Sem Retorno ao Zero *(Non Return to Zero*, NRZ), como mostrado na Figura 6. Os bits 1's são representados por impulsos retangulares de polaridade positiva, enquanto os bits 0's são representados por impulsos retangulares de polaridade negativa.

2.4 TRATAMENTO E CRIPTOGRAFIA DE SINAIS

Duas técnicas de criptografia foram utilizadas neste trabalho e com o intuito de simplificar a explicação, serão divididas nas duas seguintes subseções. Nas subseções 2.4.2 e 2.4.3, as técnicas de criptografia SPE e SS serão abordadas.

Figura 6 – Codificação de Linha NRZ.



Fonte: Autoria Própria.

2.4.1 Transformada Rápida de Fourier e Filtro RCF

Para que possamos passar os sinais gerados do domínio temporal para o domínio espectral, utilizamos o método computacional Transformada Rápida de Fourier *(Fast Fourier Transform*, FFT). Com isso, obtemos o cabeçalho $h[k]$ e o *payload* $p[k]$ no domínio espectral, $H[k]$ e $P[k]$, respectivamente. Por fim, passamos estes sinais por um filtro de Nyquist com perfil de cosseno levantado *(Raised Cossine Filter*, RCF) que é comumente usado em sistemas de comunicação digital para limitar a largura de banda do sinal transmitido, provendo proteção contra Interferências Intersimbólicas *(Intersymbol Interference*, ISI) (LATHI; DING, 2012).

A banda limitada do sinal, após passar pelo filtro RFC é obtida de acordo com a taxa de transmissão de simbolo R_{SY} do sinal e o fator de dacaimento do filtro (roll-off), r, sendo:

$$B_l = R_{SY}(1 + r)/2 \tag{1}$$

2.4.2 Codificação Espectral de Fase

Nesta subseção 2.4.2, trataremos da primeira técnica de criptografia utilizada a SPE. Neste trabalho experimental, o sinal foi amostrado em diversas componentes espectrais e, assim, uma técnica utilizando uma chave criptográfica foi aplicada para cada amostra espectral, fazendo com que o sinal a ser transmitido sofresse

uma distorção e perdesse suas características originais. Foi implementada então a função chave de fase para aplicar as distorções de fase em cada amostra. Esta função desenvolvida, gera valores de fases aleatórios $\theta[k]$ para a encriptação da k-ésima amostra espectral e não nula do *payload*. Os valores das chaves são armazenados em um vetor, compartilhados entre transmissor e receptor, e não são transmitidos concomitantemente ao sinal contendo os dados criptografados. A operação é realizada no domínio da frequência com o sinal S[k], multiplicando cada amostra espectral por cada valor complexo $e^{j\theta[k]}$ e gerando o sinal criptografado em fase C[k]:

$$S[k]e^{j\theta[k]} = C[k] \tag{2}$$

Os valores de fase $\theta[k]$ se limitam a um intervalo de 0 à 2π radianos, e são distribuídos de acordo com uma distribuição uniforme, a depender do número de amostras que representam cada símbolo.

2.4.3 Codificação por Embaralhamento

Nesta subseção 2.4.3 trataremos da segunda técnica de criptografia utilizada a SS. A operação de codificação por embaralhamento consiste em uma sequência de números que indica como a posição das amostras espectrais devem ser permutadas de acordo com uma chave K_s, que é gerada aleatoriamente (SANTOS, 2020). As amostras espectrais tem valores de fase e amplitude, nos quais apenas serão embaralhadas os valores de amplitude enquanto que a fase não se altera. Dito isto, é necessário então, o uso de uma chave de embaralhamento, para que as amostras sejam permutadas entre si, de acordo com os valores de posições atribuídos pela chave. Os

A função chave de embaralhamento funciona da forma na qual a operação foi explicada acima. Exemplificando, temos o seguinte:

Digamos que o nosso sinal tenha apenas 6 amostras espectrais:

- $U[k]$ = [0.125∠-56 0.8∠3 0.25∠5 -0.56∠25 -0.64∠30 -0.41∠29]

E a chave contendendo os seguintes valores:

- K_s = [4 3 5 6 1 2]

Logo, o nosso sinal encriptado será:

- $U_e[k]$ = [-0.56∠-56 0.25∠3 -0.64∠5 -0.41∠25 0.125∠30 0.8∠29]

Com isso o sinal está com suas amostras permutadas e embaralhadas, garantindo mais um nível de segurança ao seu sinal.

2.4.4 Aplicação das Técnicas de Criptografia e IFFT

A criptografia da carga útil do sinal por SPE em banda-base, é realizada no domínio da frequência com o sinal $H[k]$. Usa-se a chave de fase gerada, multiplicando todas as componentes espectrais da i-ésima amostra por $e^{j\theta_i}$. Logo em seguida as amostras espectrais são permutadas com a técnica de embaralhamento espectral, com a chave de embaralhamento gerada.

Após o processo de criptografia ser concluído, utilizamos o algoritmo de Transformada Rápida de Fourier Inversa *(*Inverse Fast Fourier Transform, IFFT), para retomarmos a nossa representação temporal do nosso novo sinal complexo e codificado.

3 RESULTADOS E DISCUSSÕES

Neste capítulo, iremos tratar os resultados obtidos nos experimentos realizados com as técnicas apresentadas e descritas no capítulo 2, e será dividido em três seções. A primeira seção, 3.1, apresenta os preparativos necessários da forma de onda para a sua transmissão. A segunda seção, 3.2, aborda a criação da Forma de Onda no transceptor e sua transmissão pelo enlace de RF, destacando a solução utilizada para lidar com amostras espectrais complexas. A terceira seção, 3.3, descreve o método de correlação cruzada para identificar os melhores instantes de amostragem, bem como a análise temporal e espectral dos sinais contendo os dados recebidos após a recuperação do sinal. Além disso, apresenta a análise dos bits recuperados, destacando a taxa de erro de bits *(Bit Error Rate*, BER) e investigando possíveis causas de erros.

3.1 PREPARO DA FORMA DE ONDA PARA A TRANSMISSÃO

Os métodos de criptografia mencionados anteriormente, SPE e SS, foram aplicados a sinais em banda-base.

Foram utilizados os parâmetros descritos no Quadro 2.

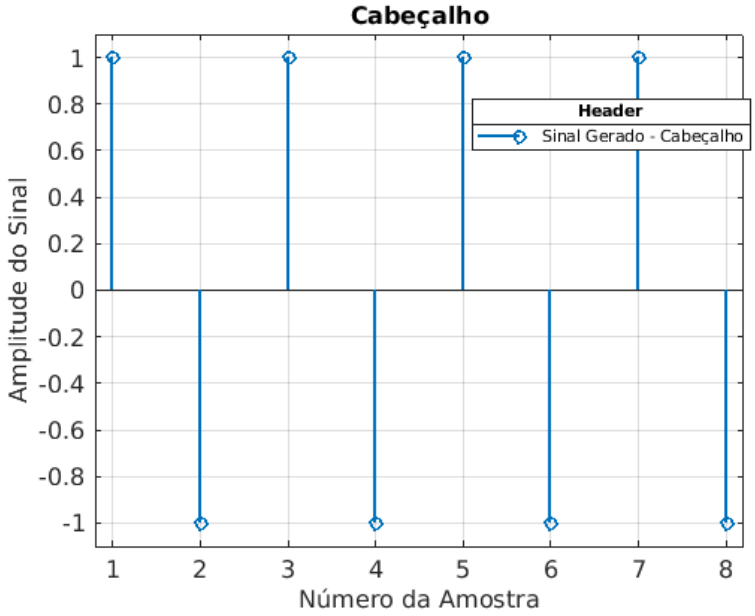
Quadro 2 – Parâmetros do Sinal Utilizado

Parâmetro	Valores
Cabeçalho	64 Símbolos
Payload	1024 Símbolos
Amostras p/ Símbolo	4
Taxa de Símbolos	1 GBaud
Roll-Off (Cabeçalho)	0,2
Roll-Off (*Payload*)	0,2

Fonte: Autoria Própria.

Foi utilizado um cabeçalho de fácil identificação, com uma sequência de amostras alternadas entre 1's e -1's, como mostrado na Figura 7, sendo este o sinal $h[k]$. Já o *payload* $p[k]$, como mencionado anteriormente, foi gerado a partir de uma PRBS, simulando valores aleatórios na carga útil do sinal. Em seguida, o cabeçalho e o *payload* são concatenados usando a função "concat", que realiza a concatenação dos valores de seus argumentos de entrada, gerando o sinal a ser transmitido.

Figura 7 – Cabeçalho Utilizado.



Fonte: Autoria Própria

$$g[k] = concat(h[k], p[k]) \tag{3}$$

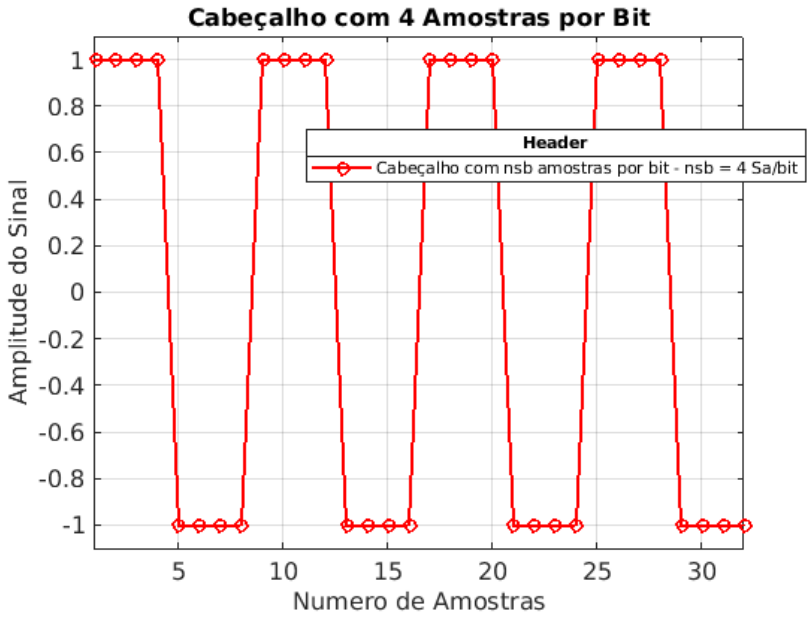
Após gerarmos o bloco que contém a informação do sinal a ser transmitido, é conveniente interpolar o sinal para aumentar o número de amostras, de modo a respeitar o teorema da amostragem no momento da transmissão. O número de amostras da informação é aumentado para 4 amostras por símbolo, conforme mostrado na Figura 8."

Logo após aumentar o número de amostras por símbolo, aplica-se a técnica de zero-padding, adicionando zeros no lugar das amostras adicionais que representam cada símbolo. No próximo passo, criptografamos o *payload* com a chave de fase gerada, resultando em um sinal complexo e criptografado em fase. Por fim, aplicamos o método de SS nas amostras usando a chave embaralhadora. As amostras espectrais são então permutadas entre si, gerando o sinal criptografado $e[k]$, apresentado na Figura 9.".

3.2 TRANSMISSÃO

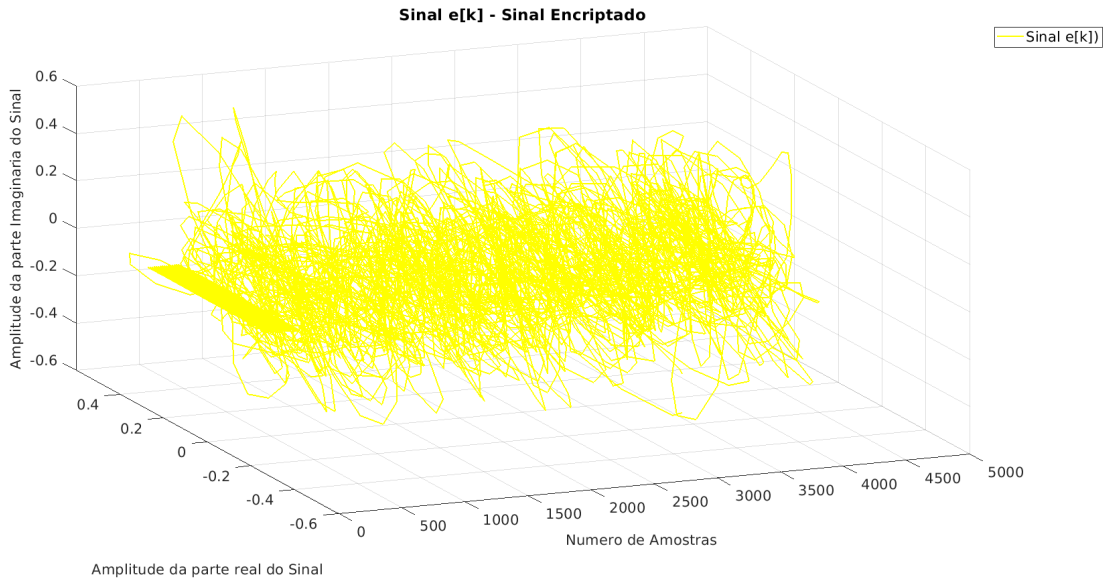
Com o sinal criptografado gerado $e[k]$, o próximo passo é criar a Forma de Onda no transceptor e transmiti-la pelo enlace de RF.O método utilizado para criar amostras complexas, foi o de transmitir a parte real pelo primeiro canal e a parte imaginária

Figura 8 – Cabeçalho com 4 amostras por simbolo.



Fonte: Autoria Própria

Figura 9 – Sinal criptografado $e[k]$.



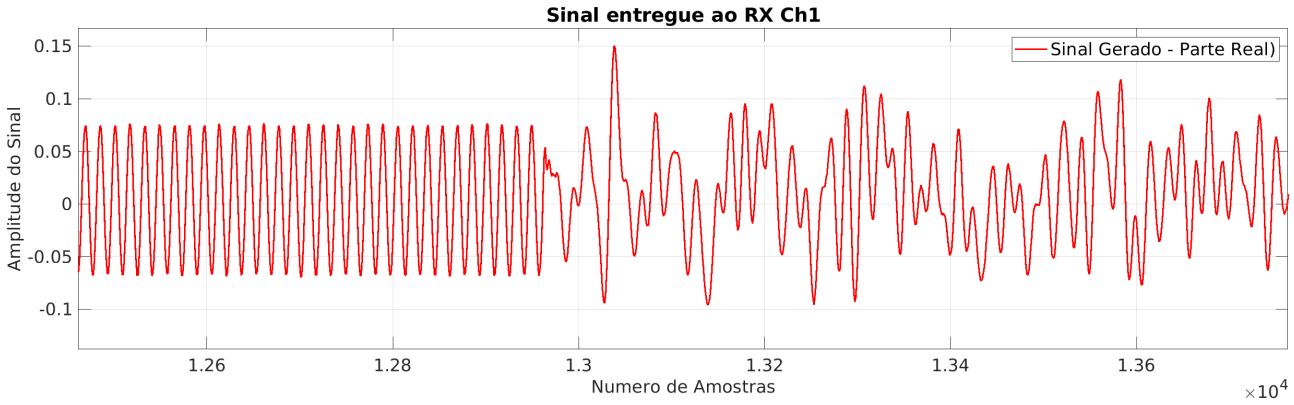
Fonte: Autoria Própria

pelo segundo canal de forma simultânea.Foi adicionado um cabeçalho às duas formas de onda para determinar o melhor instante de amostragem.

3.3 TRATAMENTO DE DADOS RECEBIDOS

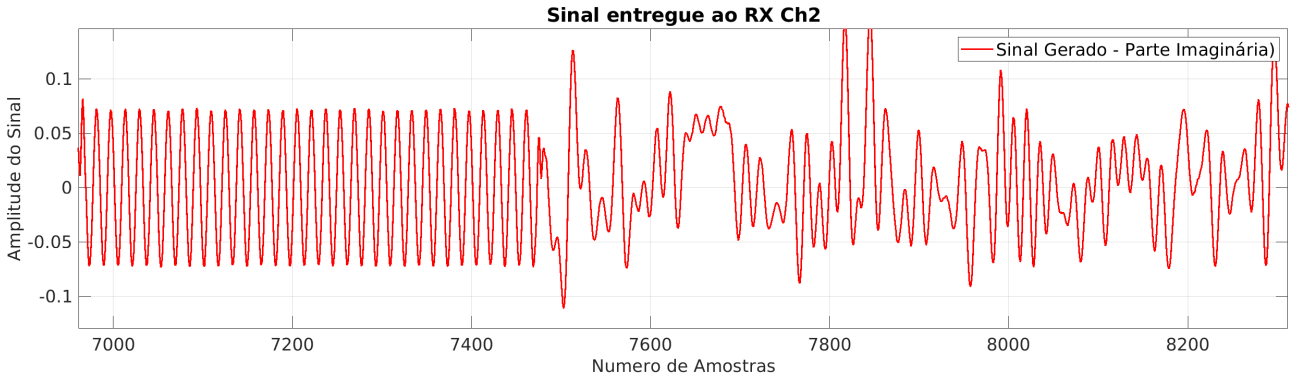
Para ter acesso aos melhores instantes de amostragem, utilizou-se o método de correlação cruzada entre o cabeçalho, previamente conhecido pelo remetente e pelo destinatário, e os sinais recebidos pelos canais 1 e 2. As Figuras Figura 10 e Figura 11 mostram uma pequena parcela dos sinais recebidos, com os melhores instantes de amostragem identificados nos canais 1 e 2, respectivamente, e os cabeçalhos claramente visíveis.

Figura 10 – Sinal Recebido no Canal 1.



Fonte: Autoria Própria

Figura 11 – Sinal Recebido no Canal 2.



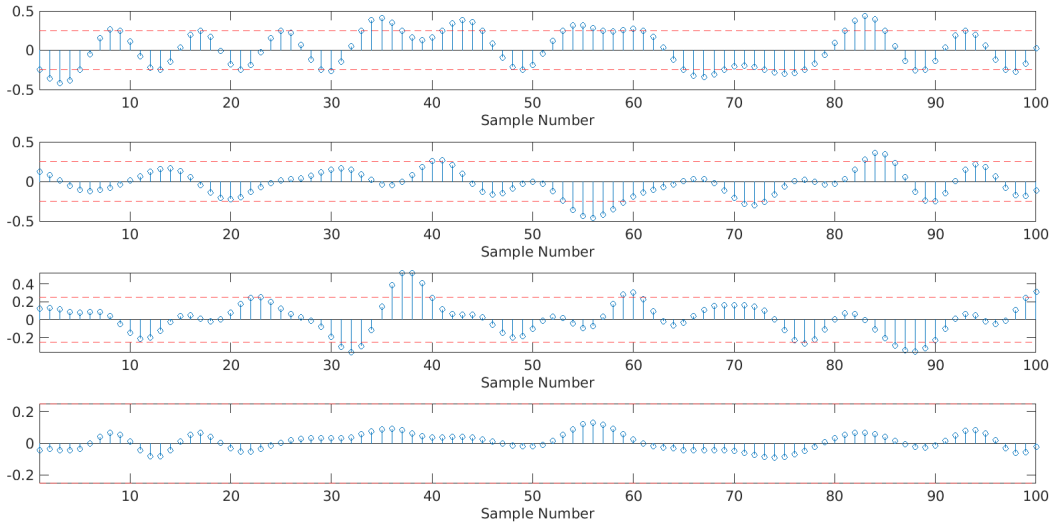
Fonte: Autoria Própria

3.3.1 Análise Temporal

Após a coleta dos dados recebidos, o sinal foi recuperado utilizando as amostras com o melhor instante de amostragem, além das chaves de fase e do embaralhamento. O sinal gerado está representado nas figuras, que mostram os resultados obtidos após

todo o processo de codificação, transmissão e decodificação. A Figura 12 apresenta o sinal discretizado a 4 amostras por símbolo, após passar pelo filtro RCF, ser codificado em fase, ter suas amostras embaralhadas e, por fim, ser recebido e descriptografado.

Figura 12 – Amostras do *Payload*, obtidas (a) após passar pelo filtro RCF, (b) após receber a codificação espectral de fase, (c) após o embaralhamento das amostras espectrais e (d) *payload* decodificado após a transmissão.



Fonte: Autoria Própria

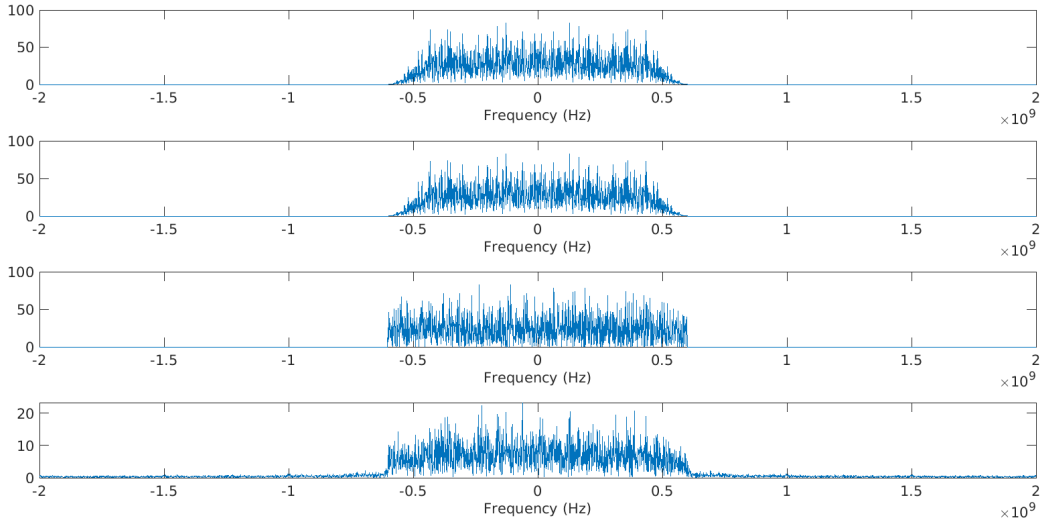
3.3.2 Análise Espectral

Nesta subseção, analisaremos os espectros de amplitude dos sinais gerados, criptografados e recebidos. A Figura 12 (a) representa o espectro de amplitude após o sinal passar pelo filtro RCF, com sua banda limitada de acordo com a taxa de transmissão de símbolos e o fator de decaimento do filtro. Na Figura 12 (b), observa-se que o espectro de amplitude do sinal, após ser criptografado, não se alterou, o que faz sentido, dado que a criptografia aplicada foi a codificação espectral de fase. Já na Figura 12 (c), percebe-se uma mudança no espectro do sinal, pois as amostras foram embaralhadas e estão fora de suas posições originais. Por fim, na Figura 12 (d), pode-se observar o espectro de amplitude do sinal recuperado.

3.3.3 Análise dos Bits Recuperados

A Figura 14 apresenta o resultado experimental obtido. Após realizar todo o tratamento de decodificação e desembaralhamento do sinal, e reduzir o número de

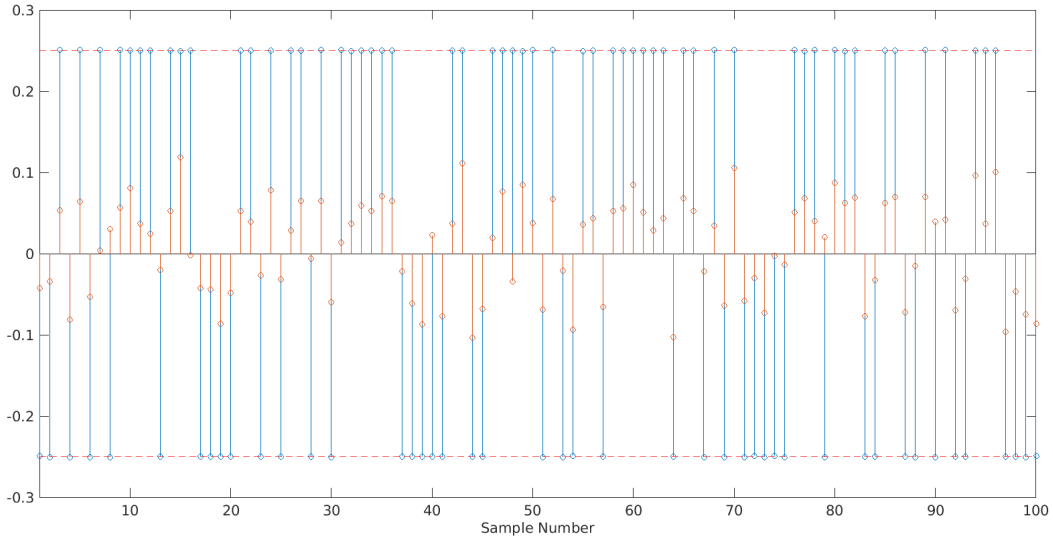
Figura 13 – Espectros de Amplitude do *Payload*, obtidos (a) após passar pelo filtro RCF, (b) após receber a codificação espectral de fase, (c) após o embaralhamento das amostras espectrais e (d) *payload* decodificado após a transmissão.



Fonte: Autoria Própria

amostras por símbolo para 1, obtivemos uma recuperação parcial do sinal, com 942 símbolos recuperados corretamente e 82 símbolos recuperados de forma incorreta, resultando em uma BER de aproximadamente 8%. O fator que contribuiu para essa alta taxa de BER foi, provavelmente, um erro na rotina implementada no MATLAB para determinar o melhor instante de amostragem. A rotina parece estar incorreta, causando essa incompatibilidade na comparação entre o sinal transmitido e o recebido. Isso ainda está sendo avaliado, o que nos traz a necessidade de continuar com testes futuros para corrigir o código, que impede a recuperação adequada do sinal.

Figura 14 – Bits recuperados e comparados com os bits originais.



Fonte: Autoria Própria

4 CONCLUSÃO

Após a realização de experimentos para verificar o desempenho de técnicas de criptografia de sinais, como a Codificação Espectral de Fase e o Embaralhamento Espectral, os resultados obtidos foram promissores, porém, com o objetivo final ainda inalcançado. A verificação experimental realizada indica que há potencial para utilização das técnicas de criptografia em sistemas reais. Os testes realizados com o transceptor e a análise dos dados recebidos após a transmissão e decodificação dos sinais criptografados revelaram uma recuperação parcial do sinal, com uma BER de aproximadamente 8%. Isso possivelmente se deve ao fato de algum erro na implementação da rotina do Código usado no MATLAB no momento de determinar o melhor instante de amostragem, e também na questão da falta de sincronização entre os transmissores, causando uma taxa muito alta de BER.

A continuidade dos experimentos e a busca por aprimoramentos nos processos de codificação e transmissão são essenciais para melhorar a recuperação dos sinais e reduzir a taxa de erro. A criptografia de sinais na camada física, desenvolvida pelo grupo de estudos da UNESP-SJBV, mostra-se uma abordagem promissora para reforçar a segurança dos dados transmitidos em redes de comunicação comerciais.

Dessa forma, os resultados obtidos neste estudo experimental abrem perspectivas para futuras pesquisas e aplicações práticas das técnicas de criptografia de sinais, visando garantir a confidencialidade e integridade das informações em ambientes de comunicação digital.

REFERÊNCIAS

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. 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.

ALURA. **Saiba o que é o modelo OSI e quais são suas camadas** Disponível em: https://www.alura.com.br/artigos/conhecendo-o-modelo-osi. Acesso em: 15 de Janeiro de 2024.

ARAÚJO, E. J. **Criptografia: dos rudimentos à atualidade**. Universidade Federal do Estado do Rio de Janeiro. Rio de Janeiro, p. 1-76. 2018.

BARBIERI, A. **TEN Gigabit Ethernet and Its "X" Factors** Cisco Systems, Inc. p. 1-10, 2005

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.

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

CARDOSO, M. T. **UTILIZAÇÃO DO GALOIS COUNTER MODE PARA PROVIMENTO DE AUTENTICAÇÃO E SINCRONIZAÇÃO POR PILOTOS EM ESTRATÉGIAS DE CRIPTOGRAFIA DE SINAIS**. Universidade Estadual Paulista "Júlio de Mesquita Filho"(UNESP). São João da Boa Vista, p. 1-49. 2022. Trabalho de Conclusão de Curso de graduação

CORNEJO, J. ; PEREZ, ; TOCNAYE, J.-L. D. B. D. L. WDM-Compatible Channel Scrambling for Secure High-Data-Rate Optical Transmissions. **Journal of Lightwave Technology**, v. 25, n. 8, p. 2081-2089, Agosto 2007.

CLOADFLARE. **O que é camada de rede? Camada de rede x camada de internet** Disponível em: https://www.cloudflare.com/pt-br/learning/network-layer/what-is-the-network-layer/. Acesso em: 22 de Junho de 2024.

DAEMEN, J.; RIJMEN, V. **The Design of Rijndael.** 1ª. ed. Heidelberg: Springer Berlin, 2001.

FERNÁNDEZ, M. P. **Computação - Rede de Computadores.** 1. ed. Editora da Universidade Estadual do Ceará – EdUECE, 2019. 192 p.

HALBOUNI, A.; ONG, L.; LEOW, M. et al. **Wireless Security Protocols WPA3: A Systematic Literature Review.** VOLUME XX, 2017. p. 3.

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

LI W., MCLERNON D., LEI J.,GHOGHO M., ZAIDI S. A. R. e HUI H., **Cryptographic Primitives and Design Frameworks of Physical Layer Encryption for Wireless Communications**, IEEE Access, vol. 7, p. 63660-63673, 2019.

NOGUEIRA, M. P. **Criptografia física por embaralhamento espectral aplicada a sinais.** Universidade Estadual Paulista Júlio de Mesquita Filho, Faculdade de Engenharia. São João da Boa Vista, p. 65. 2022.

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.

SANTOS, M. D. 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.

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

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

STALLINGS, W. **Criptografia e Segurança de Redes.** 6. ed. São Paulo: Pearson, 2014. 578 p.

ZHAO A., JIANG N., LIU S., ZHANG Y. e QIU K., **Physical Layer Encryption for WDM Optical Communication Systems Using Private Chaotic Phase**

Scrambling, in Journal of Lightwave Technology, vol. 39, no. 8, p. 2288-2295, 2021.