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

GABRIEL INÁCIO DELLA VECCHIA GUIMARÃES

CRIPTOGRAFIA DE CAMADA FÍSICA PARA SINAIS OFDM

SÃO JOÃO DA BOA VISTA
2020

GABRIEL INÁCIO DELLA VECCHIA GUIMARÃES

CRIPTOGRAFIA DE CAMADA FÍSICA PARA SINAIS OFDM

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

Orientador: Prof. Dr. Marcelo Luís Francisco Abbade
Co-Orientador: Prof. Dr. Ivan Aritz Aldaya Garde

SÃO JOÃO DA BOA VISTA
2020

G963c

Guimarães, Gabriel Inácio Della Vecchia
Criptografia de camada física para sinais OFDM / Gabriel Inácio Della Vecchia Guimarães. -- São João da Boa Vista, 2020
41 p. : il., tabs.

Trabalho de conclusão de curso (Bacharelado - Engenharia de Telecomunicações) - Universidade Estadual Paulista (Unesp), Câmpus Experimental de São João da Boa Vista, São João da Boa Vista
Orientador: Marcelo Luís Francisco Abbade
Coorientador: Ivan Aritz Aldaya Garde

1. Criptografia. 2. Codificação. 3. Multiplexação. 4. Telecomunicações. I. Título.

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

Essa ficha não pode ser modificada.

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

TRABALHO DE CONCLUSÃO DE CURSO

CRIPTOGRAFIA DE CAMADA FÍSICA PARA SINAIS OFDM

Aluno: Gabriel Inácio Della Vecchia Guimarães
Orientador: Prof. Dr. Marcelo Luís Francisco Abbade

Banca Examinadora:

- Marcelo Luís Francisco Abbade (Orientador)
- Cintya Wink de Oliveira Benedito (Examinadora)
- Edgar Eduardo Benitez Olivo (Examinador)

A ata da defesa com as respectivas assinaturas dos membros encontra-se no prontuário do aluno (Expediente nº 16/2019)

RESUMO

Neste trabalho, a implementação de uma técnica de criptografia de sinais baseada em codificação espectral junto a técnica de multiplexação por divisão de frequências ortogonais (*orthogonal frequency division multiplexing*, OFDM) é realizada e seu desempenho analisado por meio de simulações numéricas. A técnica de criptografia é uma adaptação da técnica de codificação espectral de fase (*spectral phase encoding*, SPE), a qual particiona um sinal em diversas fatias espectrais, e altera algumas de suas propriedades. A adaptação feita visa alterar também a amplitude de cada fatia de forma a aumentar a robustez da criptografia como um todo. Foram implementados também dois formatos diferentes de modulação para a transmissão, o 16-QAM retangular e o 16-QAM estrela de duplo anel (*dual-ring star 16-QAM,* DRS-16-QAM*)*. Após a implementação, foram feitas simulações com o objetivo de analisar o desempenho do sistema com um sinal sendo transmitido por um canal com ruído gaussiano branco aditivo (*additive white gaussian noise,* AWGN). Os resultados mostraram que a criptografia é robusta, com o sinal criptografado apresentando taxa de erro de bit (*bit error rate*, BER) de valor próximo a 0,5, o maior valor possível. Os resultados também mostraram que a utilização da técnica DRS-16-QAM é ideal para este tipo de sistema, pois possui um compromisso satisfatório entre a BER e a variação da relação sinal-ruído (*signal-to-noise ratio*, SNR) do canal, quando comparado com a modulação 16-QAM retangular.

Palavras-chave: Criptografia de sinais, multiplexação ortogonal por divisão de frequência, codificação espectral de fase, 16-QAM estrela de duplo-anel, 16-QAM retangular.

ABSTRACT

In this work, the implementation of a spectral-based signal encryption technique along with the orthogonal frequency division multiplexing (OFDM) technique is performed and its performance is analyzed using numerical simulations. The cryptography technique is an adaptation of the spectral phase encoding (SPE) technique, which partitions a signal into several spectral slices, and changes some of its properties. The adaptation made also aims to change the amplitude of each slice in order to increase the strength of the cryptography as a whole. Two different modulation formats for transmission were also implemented, the rectangular 16-QAM and the dual-ring star 16-QAM (DRS-16-QAM). After implementation, simulations were carried out in order to analyze the performance of the system being transmitted through a channel with additive white gaussian noise (AWGN). The results induced that the encryption is robust, with the encrypted signal at a bit error rate (BER) extremely close to the maximum possible value. They also show us that the use of the DRS-16-QAM technique is ideal for this type of system, as it has a satisfactory compromise between BER and the variation of the signal-to-noise ratio (SNR) of the channel, when compared with rectangular 16-QAM modulation.

Keywords: Signal encryption, frequency division orthogonal multiplexing, spectral phase encoding, double-ring star 16-QAM, rectangular 16-QAM.

Lista de Símbolos

A_{crip}	Vetor real de módulos de amplitude criptografados
A_{dec}	Vetor real de módulos de amplitude descriptografados
A_k	Vetor real indexador das amplitudes de entrada
B_k	Vetor real indexador de amplitudes aleatórias (Chave)
C_k	Vetor real indexador do sinal criptografado no transmissor
C'_k	Vetor real indexador do sinal criptografado recebido
D_k	Vetor real indexador do sinal de amplitudes descriptografado
k	Número de diferentes módulos de amplitude do sinal
n_s	Número de fatias espectrais do sinal
φ_n	Fases do sinal fatiado espectralmente
S_{crip}	Vetor complexo do sinal criptografado em fase e amplitude
S_{dec}	Vetor complexo do sinal descriptografado em fase e amplitude
θ_{chave}	Vetor real de fases aleatórias (Chave)
θ_{crip}	Vetor real de fases criptografado

Índice de Acrônimos

AWGN	Ruído aditivo gaussiano e branco
BER	Taxa de erro de bit
CP	Prefixo cíclico
dB	Decibel
DFT	Transformada discreta de Fourier
DRS-16-QAM	16-QAM estrela de duplo anel
DSP	Processamento digital de sinais
FDM	Multiplexação por divisão de frequência
ISI	Interferência intersimbólica
OFDM	Multiplexação por divisão de frequências ortogonais
OSI	Interconexão de sistemas abertos
PSK	Modulação por deslocamento de fase
QAM	Modulação de amplitude em quadratura
QC	Criptografia quântica
QKD	Distribuição de chave quântica
SE	Criptografia de sinais
SNR	Relação sinal-ruído
SPAE	Codificação espectral de fase e amplitude
SPDE	Codificação espectral de fase e atraso
SPE	Codificação espectral de fase

Índice de Figuras

Índice de Tabelas

Sumário

1. Introdução

O número de pessoas que está conectado por sistemas de telecomunicação cresce diariamente em conjunto com o surgimento de novas tecnologias. Computadores, celulares, relógios, aparelhos eletrodomésticos e outros dispositivos, necessitam cada vez mais de sistemas seguros, estáveis e confiáveis. Para aumentar a confiabilidade em transmissões, o uso de técnicas de criptografia é recomendado [1].

A primeira seção deste capítulo é dedicada a abordar os conceitos referentes a criptografia de dados e de sinais, além da motivação para realização do presente trabalho. A segunda seção apresentará uma revisão bibliográfica das principais técnicas de criptografia de sinais. A seção três apresentará as principais contribuições deste trabalho e por último, a quarta seção apresentará a organização deste trabalho.

1.1. Conceitos Criptográficos e Motivação

Em 1948, Shannon publicou um artigo chamado "*A Mathematical Theory of Cryptography"* [2], o qual descreve matematicamente conceitos de criptografia e duas propriedades importantíssimas, que quando cumpridas, podem qualificar uma criptografia segura. Essas propriedades foram nomeadas difusão e confusão, e quando utilizadas, impedem que o uso de criptoanálises estatísticas e outras técnicas de descriptografia sejam utilizadas com sucesso para quebrar uma cifra.

A propriedade da difusão postula que se alterarmos em um bit os dados de uma informação de entrada, os dados dessa informação quando criptografada devem variar em aproximadamente 50% dos bits. Assim, cria-se uma descorrelação entre a informação de entrada e a informação cifrada, dificultando uma possível tentativa de um intruso (*eavesdropper)* descobrir a informação original.

A segunda propriedade, a confusão, serve para obscurecer a relação entre a informação criptografada e a sua chave. Ela requer que cada bit da informação criptografada dependa de vários bits na chave. Assim, por mais que um possível intruso tenha controle sobre as estatísticas dos dados da informação, ele não poderá deduzir a chave, pois a maneira utilizada para produção da chave é extremamente complexa e não possui correlação com a informação criptografada [3].

A técnica de criptografia mais utilizada atualmente é a criptografia dos dados, ou seja, os bits armazenados em um computador, por exemplo. Este tipo de criptografia já é consolidado nos sistemas de comunicação atuais. As técnicas de criptografia de dados são implementadas nas camadas superiores do modelo para interconexão de sistemas abertos (*open system interconnection*, OSI).

Em sistemas de comunicação, eventualmente bits de uma mensagem são convertidos para sinais, que também podem ser criptografados. O uso de técnicas de criptografia de sinais, especificamente na camada física do modelo OSI, pode aumentar a segurança significativamente, pois ao criptografarmos a camada física, a demais camadas também são criptografadas (princípio da modularidade). Outro ponto, é a necessidade de proteger o sinal durante a sua propagação, visto que os proprietários da rede não necessariamente são os proprietários das informações que trafegam por elas.

O uso de técnicas de modulação avançadas como a OFDM é muito popular atualmente, pois possibilita alta eficiência espectral, robustez contra interferência intersimbólica (*intersymbol interference*, ISI) e desvanecimentos. Isso torna possível a utilização da técnica OFDM por diversos padrões presentes em sistemas de telecomunicação atuais, como *IEEE 802.11a/g/n*, *IEEE 802.16 WiMAX* e *Long-Term Evolution* (LTE).

Neste trabalho, o uso de técnicas de criptografia de camada física baseadas em codificação espectral em conjunto com a técnica de modulação OFDM é analisado por meio de simulações numéricas. O trabalho tem o foco principal na implementação da técnica de criptografia de sinais, existindo a possiblidade de utilização tanto em sistemas de transmissão óticos como em sistemas de transmissão sem-fio. Apesar dos conceitos dos conceitos de difusão e confusão serem importantes para atestar a segurança de uma técnica de criptografia, eles não foram testados neste trabalho, pois como citado anteriormente, o trabalho tem o foco principal na implementação da técnica de criptografia. No melhor de nosso conhecimento e após exaustiva busca na literatura disponível verificou-se que ainda não existem estudos deste tipo, circunstancia favorável para o desenvolvimento de uma pesquisa.

1.2. Trabalhos relacionados

Existem diversas técnicas promissoras sendo desenvolvidas que podem ser utilizadas para a criptografia de sinais (*signal encryption*, SE). Podemos citar, com precisão, que a mais segura dentre elas é a criptografia quântica (*quantum cryptography,* QC), uma vez que ela possui o recurso único de detectar a ação de um intruso. No entanto, sua utilização ainda não é totalmente prática, visto que a taxa de transmissão de sinais criptografados quanticamente é bem inferior ao que se é praticado comercialmente [4]. Podemos citar também a técnica de criptografia caótica, na qual já existem estudos aplicados a sistemas de transmissão OFDM [5,6,7].

As principais referências deste trabalho estão relacionadas a técnica de criptografia de camada física baseada em codificação espectral. Esta técnica propõe que um sinal seja dividido em diversas fatias espectrais, e após isso, técnicas para alteração das propriedades do sinal são aplicadas. Como exemplo, temos a técnica de codificação espectral de fase (*spectral phase encoding, SPE)* [8], que visa alterar a fase de cada fatia e seu funcionamento será explicado detalhadamente no Capítulo 3. Caso seja alterada a fase e aplicado um atraso em cada fatia, a técnica é a de codificação espectral de fase e de atraso (*spectral phase and delay encoding*, SPDE) [9]. Outra importante técnica baseada em codificação espectral é a de embaralhamento intercanal (*shuffling)* [10], na qual efetua um embaralhamento entre as fatias de dois ou mais sinais diferentes.

Existem algumas dificuldades, no caso das técnicas de SE baseadas em codificação espectral, serem aplicadas em redes ou enlaces totalmente óticos, uma vez que obter fatias com banda estreita é algo muito complexo. Uma forma seria a criação das fatias por meio de filtros óticos. No entanto, dispositivos como esses ainda não estão disponíveis comercialmente, o que torna a investigação deste tipo de implementação dificultosa.

Uma solução para a realização da criptografia de sinais que trafegam em meios óticos é a utilização da criptografia por meio de processamento digital de sinais (*digital signal processing,* DSP). Isso é possível através da aplicação da criptografia nos sinais em banda-base, e em seguida, realizar uma conversão destes sinais para o domínio ótico através de algum processo de modulação ótica.

1.3. Contribuições e Organização do Trabalho

Este trabalho tem como objetivo principal a implementação da técnica de criptografia de camada física por codificação espectral a um sistema de transmissão OFDM utilizando duas variações da modulação 16-QAM. A técnica de criptografia implementada baseia-se em SPE com a adição de um sistema que embaralha as amplitudes das fatias espectrais. Chamaremos esta técnica de codificação espectral de fase e amplitude (*spectral phase and amplitude encoding*, SPAE). O código que realiza a criptografia/descriptografia foi desenvolvido e testado através da plataforma MATLAB® e inserido ao *software* que realiza a modulação/demodulação OFDM, na qual parte deste software foi desenvolvido originalmente em [11]. Além disso, foram utilizados dois formatos diferentes de modulação 16-QAM, a modulação 16-QAM Retangular e a modulação DRS-16-QAM [12].

Os demais capítulos deste trabalho estão organizados da seguinte maneira:

- **Capítulo 2**: Neste capítulo apresenta-se um breve histórico da técnica OFDM, bem como sua fundamentação teórica e os diferentes esquemas de modulação utilizados no trabalho.
- **Capítulo 3**: A fundamentação teórica da técnica SPE será abordada neste capítulo, bem como a sua implementação junto a técnica OFDM.
- **Capítulo 4:** Neste capítulo são apresentados os resultados obtidos após a implementação da criptografia junto ao sistema de transmissão OFDM.
- **Capítulo 5:** Finalmente, as conclusões deste trabalho são apresentadas.

2. OFDM e Modulação 16-QAM

Neste capítulo abordaremos inicialmente, na primeira seção, um breve resumo cronológico da técnica OFDM. Em seguida, na Seção 2, será apresentada a fundamentação teórica referente a OFDM, explicando os principais conceitos referentes a técnica, inserção de prefixo cíclico e o mapeamento das subportadoras. Na terceira seção serão apresentados os formatos de modulação 16-QAM utilizados neste trabalho.

2.1. Cronologia da OFDM

Os sistemas de multiportadoras surgiram na década de 50 com a criação da multiplexação por divisão de frequência (*frequency division multiplexing,* FDM). Nesta época, a FDM era largamente utilizada para fins militares em comunicações de alta frequência, no entanto a complexidade relativa ao sincronismo das portadoras impactava a implementação da técnica [13].

O conceito da OFDM surge em 1966 por meio de uma publicação de Chang [14] que descrevia a transmissão multicanal de sinais limitados em banda utilizando a sobreposição espectral ortogonal de sinais multifrequência na comunicação de dados. Uma das maiores contribuições para a OFDM foi a de Weinstein e Ebert [15] em 1971, com a ideia de usar a transformada discreta de Fourier (*discrete Fourier transform,* DFT) na transmissão e recepção de sinais OFDM, reduzindo de maneira significativa a complexidade de elaboração dos modens, pois eliminou a necessidade da utilização de bancos osciladores analógicos no sistema.

Uma solução para o problema da conservação da ortogonalidade nos sistemas OFDM foi apresentada em 1980, por Peled e Ruiz [16], com a introdução do conceito de prefixo cíclico (*cyclic prefix*, CP), como é chamado de maneira usual. Esta técnica estende o período de símbolo OFDM ciclicamente ao longo do intervalo de guarda ao invés de utilizar intervalos de guarda vazios, ou seja, sem sinal. Com isso, a área de atuação da técnica OFDM pôde ser ampliada e inserida e diferentes cenários, como as comunicações móveis em 1985 [17].

2.2. Fundamentação Teórica

A técnica OFDM é considerada uma evolução da técnica FDM na qual, ao invés de utilizar bandas de guarda para a separação das subportadoras no receptor, utiliza-se uma sobreposição do espectro das subportadoras [18].

Em sistemas de transmissão de portadora única, normalmente, os símbolos são enviados em sequência por meio de uma única portadora, que está modulada na taxa de símbolos da fonte de informação, com o seu espectro ocupando toda a faixa de frequências disponível. Em contrapartida, a técnica OFDM realiza uma transmissão de dados de modo paralelo em diversas subportadoras. As subportadoras podem utilizar modulação por deslocamento de fase (*phase shift keying*, PSK) ou modulação de amplitude em quadratura (*quadrature amplitude modulation*, QAM). Dada uma largura de banda disponível, as taxas de transmissão por subportadora são tão baixas quanto maior o número de subportadoras. Com essa diminuição na taxa de transmissão, que ocorre devido ao aumento na duração dos símbolos transmitidos em cada subportadora, a sensibilidade à seletividade em frequência (dispersão no tempo) em sistemas de transmissão sem-fio, que é causada pelo efeito do multipercurso e pela interferência entre símbolos, também é diminuída [18].

Em um sistema OFDM, as frequências das subportadoras devem ser cuidadosamente selecionadas para que sejam alocadas na posição dos nulos espectrais das demais, configurando assim uma condição de ortogonalidade entre elas. Desta maneira, a OFDM não necessita de uma banda de guarda entre as portadoras, o que possibilita uma alta eficiência espectral. Outro benefício, proveniente da sobreposição espectral, é uma menor necessidade de banda, principalmente em relação a técnica FDM, que utiliza toda a faixa disponível. Assim, uma quantidade maior de informação pode ser utilizada, conforme mostra a Fig. 1, onde se observa a diferença do uso de banda entre as duas técnicas.

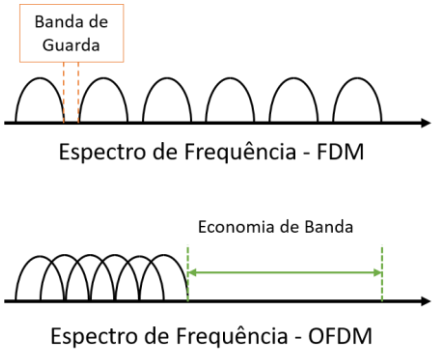


Figura 1- Diferença de uso de banda entre as técnicas de modulação FDM e OFDM. Fonte: [15].

Para que seja obtido um grau de sincronismo satisfatório entre o transmissor e receptor, em sistemas OFDM, são inseridas subportadoras pilotos que geram um sinal de referência para o receptor. Além disso, as subportadoras pilotos não são moduladas e suas posições são conhecidas pelo receptor, possibilitando a estimativa da função de transferência do canal utilizado na transmissão. Assim, com a resposta em frequência do canal estimada, pode-se realizar uma equalização do canal e compensar possíveis variações de fase e amplitude das subportadoras, que são causadas pelos efeitos da dispersão ou do multipercurso.

2.2.1. Prefixo Cíclico

Em sistemas de transmissão em que um sinal viaja por um canal dispersivo, as componentes frequenciais do sinal viajam em velocidades de fase diferentes, o que pode ocasionar um espalhamento gerado pela dispersão e, consequentemente, o surgimento de ISI. Em sistemas OFDM, a ISI é uma grande geradora de falhas no processo de ortogonalidade, o qual é fundamental para a concepção deste tipo de sistema. Para contornar a ISI, a utilização da técnica do CP é recomendada.

A técnica do CP consiste na adição de um conjunto de amostras presentes no final de um sinal ao início do mesmo. Com isso, a ISI é evitada ao custo de um aumento significativo no tamanho do símbolo utilizado. Assim, o receptor recebe um trecho do sinal que é totalmente livre de ISI, contendo toda a informação necessária para a demodulação [19]. A Fig. 3 representa a técnica do CP.

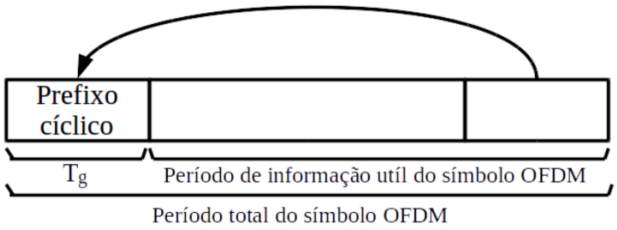


Figura 2 – Símbolo OFDM com a adição do prefixo cíclico. Fonte: [18].

2.2.2. Mapeamento de Subportadoras

Em sistemas de transmissão OFDM implementados digitalmente, cada subportadora é modulada em PSK ou QAM, possuindo vários bits mapeados em cada subportadora. Estes conjuntos de bits são mapeados como símbolos de valor complexo representando os pontos em

um diagrama de constelação. Este diagrama é a representação de um sinal modulado digitalmente em um plano complexo, onde o seu eixo horizontal (real) representa componentes do sinal em fase e o seu eixo vertical (imaginário) representa as componentes do sinal em quadratura. Então dependendo das características do sinal utilizado no sistema e do tipo de modulação, a constelação terá um formato e número de pontos distintos. Observa-se também que durante a recepção de um sinal, quanto maior a dispersão dos símbolos no diagrama, maior é a possibilidade de haver degradação do sinal utilizado.

Em sistemas OFDM, durante o mapeamento do sinal, normalmente utiliza-se a codificação Gray. Nesta técnica de codificação a diferença dos códigos entre dois pontos adjacentes é dada pela variação de um bit. A principal motivação para a utilização da codificação Gray em sistemas OFDM é a redução da taxa de erro de bits. [20]

Cada ponto do diagrama de constelação representa uma codificação em dados binários. A Fig. 3 mostra um diagrama de constelação de um mapeamento 16-QAM, onde existem dezesseis pontos de constelação distribuídos entre quatro quadrantes do plano usando uma codificação Gray nos pontos.

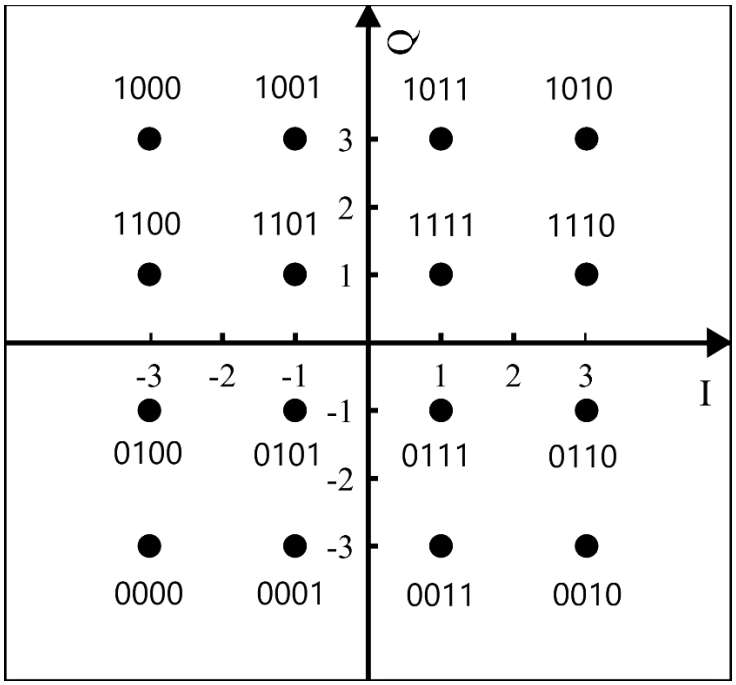


Figura 3 – Exemplo de um diagrama de constelação de um sinal 16-QAM Retangular mapeado usando a codificação Gray. Fonte: O Autor.

2.3. 16-QAM Retangular e 16-QAM Estrela de Duplo Anel

Existem muitas possibilidades para projetar uma constelação de sinal 16-QAM. Os dois principais formatos são o 16-QAM de formato retangular e o 16-QAM de formato estrela. Nesta Seção iremos abordar como projetar de maneira ótima estes formatos de constelação.

2.3.1. DRS-16-QAM

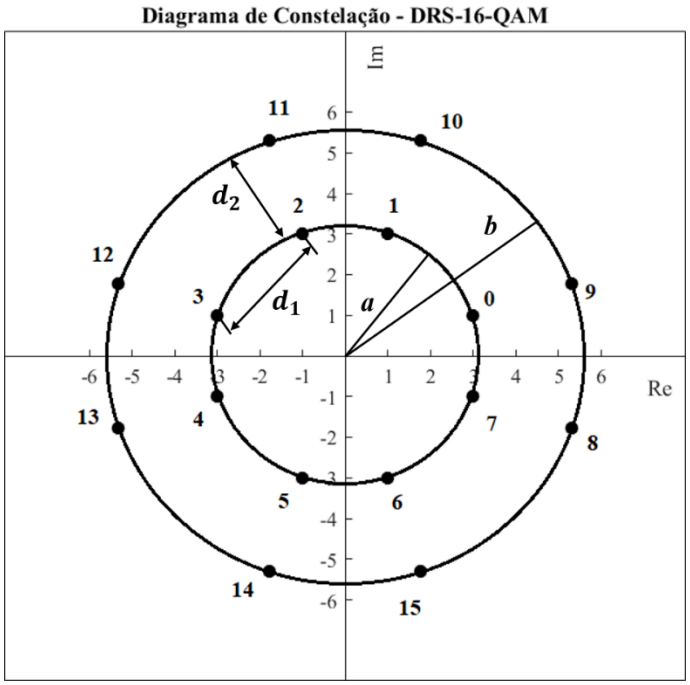


Figura 4 - Arranjo teórico do diagrama de constelação da modulação 16-QAM Estrela de Duplo Anel (DRS-16-QAM). Fonte: [21].

O diagrama de constelação para a o DRS-16-QAM com codificação em decimal pode ser observado na Fig. 5. Os valores correspondentes em Gray e Binário podem ser encontrados na Tabela 1 contida na Seção 2.3.3. Seus símbolos estão distribuídos de maneira uniforme sobre dois anéis e as diferenças de fase entre os símbolos vizinhos no mesmo anel são iguais ($\pi/4$). Entre dois níveis de amplitude e oito possíveis fases, existem inúmeras maneiras de formas essa constelação [21].

A proporção dos anéis (*Ring Ratio*, RR) para esta constelação pode ser definida como RR = b/a, onde a e b são os raios do primeiro e do segundo anel, respectivamente. A RR pode ser ajustada para diferentes valores de forma a otimizar o desempenho em transmissões [21].

Teoricamente, a melhor RR é definida com o objetivo de minimizar a probabilidade erros em um canal AWGN maximizando a distância mínima d_{min} entre símbolos vizinhos [22].

Para a 16-QAM estrela a distância mínima d_{min} é maximizada quando:

$$d_1 = d_2 = b - a = d_{min} \tag{1}$$

em que d_1 representa a menor distância entre pontos de constelação no mesmo anel, d_2 representa a menor distância entre o anel externo e o interno, a representa o raio do anel interno e b representa o raio do anel externo.

Através de manipulação trigonométricas, podemos admitir que [21]:

$$d_{min} = 2asen(\frac{\pi}{8}) \tag{2}$$

O que nos leva a uma proporção de anel óptima RR_{opt} de:

$$RR_{opt} = \frac{b}{a} = \frac{d_{min} + a}{a} = \frac{2asen(\frac{\pi}{8}) + a}{a} = 1{,}77 \tag{3}$$

2.3.2. 16-QAM Retangular

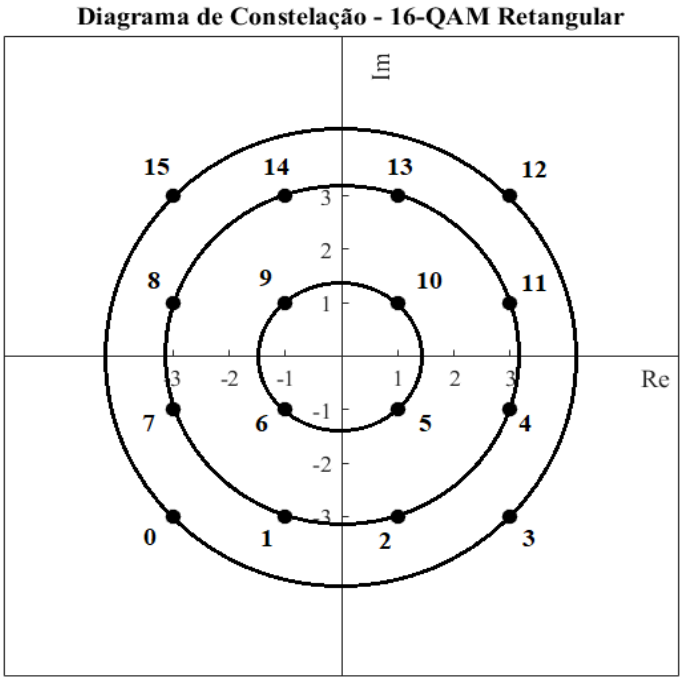


Figura 5 - Arranjo teórico do diagrama de constelação da modulação 16-QAM Retangular. Fonte: O Autor.

Na Fig. 6 podemos observar o diagrama de constelação de um sinal 16-QAM Retangular com codificação decimal. Os valores de cada ponto da constelação em Gray e Binário podem ser encontrados na Tabela 2 contida na próxima Seção. Nesta constelação, os dezesseis símbolos são equidistantes dos seus vizinhos mais próximos e possuem doze fases diferentes [23], isto é, três fases por quadrante divididos em três anéis. As diferenças de fase entre símbolos vizinhos nos círculos interiores e exteriores são iguais ($\pi/2$), em contrapartida, no círculo do meio as fases são diferentes (37º ou 53º).

2.3.3. Mapeamento dos Símbolos QAM

A primeira etapa no processo da transmissão é a de mapeamento dos bits do sinal de entrada em símbolos QAM. Em nosso sistema é implementada uma função que realiza o mapeamento destes bits em símbolos e os codifica em Gray, sem a necessidade de nenhuma *toolbox* do MATLAB®.

Na Tabela 1 podemos observar como foram distribuídos os símbolos pelo diagrama de constelação da modulação DRS-16-QAM. Observa-se que a $RR_{opt,}$ abordada na seção 2.3.1. foi utilizada entre os dois anéis que compõem o diagrama para que a probabilidade de erros fosse diminuída. A Tabela 2 refere-se ao mapeamento realizado na modulação 16- QAM Retangular.

Tabela 1 – DRS-16-QAM.

Decimal	Binário	Gray	Complexo
0	0000	0000	3+i
1	0001	0001	1+3i
2	0010	0011	-1+3i
3	0011	0010	-3+i
4	0100	0110	-3-i
5	0101	0111	-1-3i
6	0110	0101	1-3i
7	0111	0100	3-i
8	1000	1100	1,77(3-i)
9	1001	1101	1,77(3+i)
10	1010	1111	1,77(1+3i)
11	1011	1110	1,77(-1+3i)
12	1100	1010	1,77(-3+i)
13	1101	1011	1,77(-3-i)
14	1110	1001	1,77(-1-3i)
15	1111	1000	1,77(1-3i)

Tabela 2 - 16-QAM Retangular.

Decimal	Binário	Gray	Complexo
0	0000	0000	-3-3i
1	0001	0001	-1-3i
2	0010	0011	1-3i
3	0011	0010	3-3i
4	0100	0110	3-i
5	0101	0111	1-i
6	0110	0101	-1-i
7	0111	0100	-3-i
8	1000	1100	-3+i
9	1001	1101	-1+i
10	1010	1111	1+i
11	1011	1110	3+i
12	1100	1010	3+3i
13	1101	1011	1+3i
14	1110	1001	-1+3i
15	1111	1000	-3+3i

3. Criptografia de Camada Física e Implementação

O presente capítulo abordará em sua primeira seção um desenvolvimento teórico do funcionamento da técnica de criptografia de camada física baseada em codificação espectral SPE, que serviu de base para a técnica implementada neste trabalho. Na segunda seção a implementação da técnica de criptografia SPAE, desenvolvida neste trabalho, será discutida.

3.1. Criptografia baseada em Codificação Espectral de Fase (SPE)

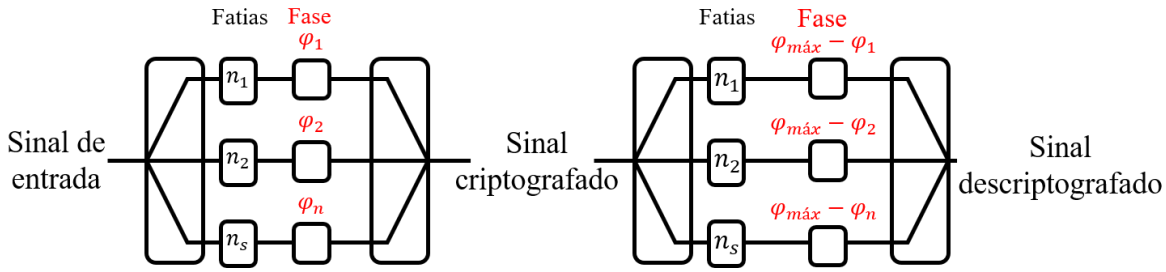


Figura 6 - Esquematização da encriptação (a) e desencriptação (b) de um sinal por SPE. Fonte: [24].

Na técnica SPE um sinal é divido n_s fatias espectrais e então, é aplicado um desvio de fase φ_n em cada uma das fatias. As fatias são então multiplexadas, formando um novo sinal, que já está criptografado e possui a mesma banda do sinal de entrada. A chave para a descriptografia é formada pelo conjunto dos desvios de fase adicionados a cada fatia. Após ser propagado pelo canal, o sinal criptografado chega ao receptor autorizado, onde a chave criptográfica é conhecida.

A chave deve ser trocada entre transmissor e receptor, e para isso, pode usar a técnica de distribuição de chave quântica (*quantum key distribuition*, QKD) via satélite [25]. Após receber o sinal criptografado e possuindo a chave, o receptor divide o sinal criptografado no mesmo número de fatias utilizado pelo transmissor e aplica o desvio de fase de maneira complementar a cada fatia. Por fim, as fatias espectrais são então multiplexadas novamente e o sinal original é recuperado ao custo de uma determinada penalidade de propagação. A Fig. 4 ilustra esquematicamente o processo da SPE.

3.2. Implementação da técnica SPAE

Esta sessão dedica-se a apresentação da implementação da técnica de criptografia de sinais SPAE a um sistema de transmissão OFDM. A primeira parte irá abordar o processo de criptografia do sinal e a segunda parte o processo de descriptografia.

3.2.1. Criptografia

A criptografia de sinais SPAE foi desenvolvida baseando-se em um modelo de criptografia por codificação espectral de fase (SPE) e na técnica OFDM. A criptografia é implementada durante o processo de modulação OFDM, especificamente, conforme a Fig. 7, após o mapeamento dos bits de entrada em símbolos complexos. A técnica de criptografia consiste na divisão do sinal em n_s amostras espectrais de valor complexo (fatias) que são armazenadas em um vetor. Em seguida, é gerado um vetor real contendo n_s valores de fase aleatórios, chamado de θ_{chave}, que será utilizado como a chave da criptografia. Após isso, as fases de cada fatia são somadas as fases aleatórias da chave. Os valores resultantes são armazenados em um vetor complexo chamado θ_{crip}.

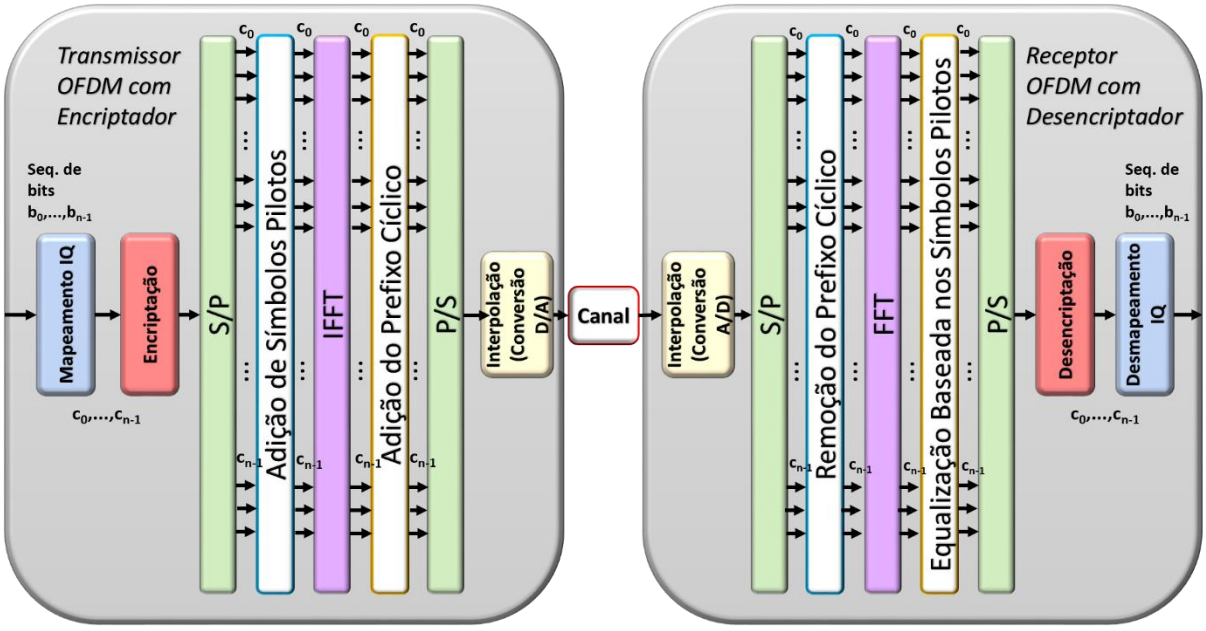


Figura 7 - Diagrama de blocos do Transmissor/Receptor OFDM com Encriptador/Desencriptador. Fonte: O Autor.

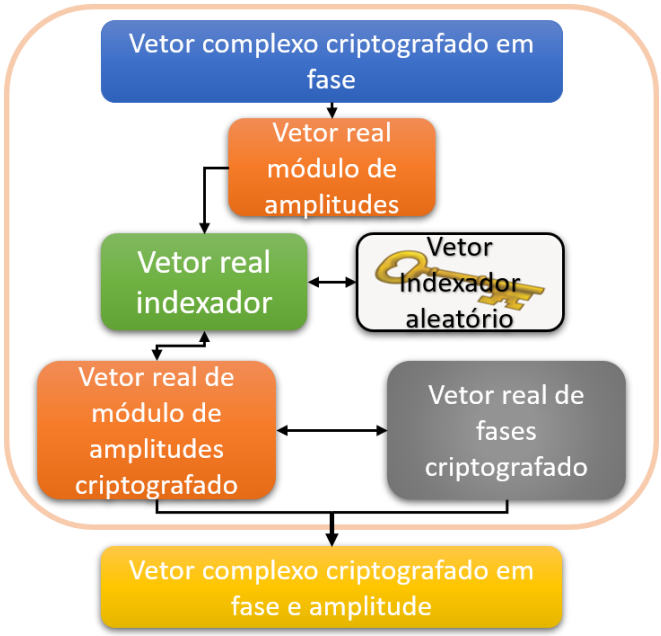


Figura 8 - Esquematização do processo de criptografia das amplitudes do sinal. Fonte: O Autor.

A segunda parte da criptografia do sinal consiste na alteração aleatória dos valores de amplitude das fatias já criptografadas em fase. Para isso, conforme a Fig. 8, o vetor resultante da criptografia em fase é separado em dois vetores reais, contendo os valores de módulo de amplitude e os valores de fase, respectivamente. Então, um vetor real indexador A_k, composto de n_s números inteiros com valores de 0 a *k-1,* em que k representa o número de diferentes módulos de amplitude do sinal, é criado. Os valores desse vetor são relacionados a cada módulo de amplitude do sinal. De forma correspondente, outro vetor real indexador, chamado de $B_{k,}$ e composto de n_s números inteiros com valores de 0 a *k-1* é criado. No entanto, esses valores estarão organizados de maneira aleatória. Este vetor indexador aleatório B_k será utilizado como chave da criptografia dos da amplitude do sinal. Então, utilizando os dois vetores indexadores A_k *e* B_k, um vetor resultante C_k é dado por:

$$C_k = (A_k + B_k) mod\ k \tag{4}$$

no qual A_k corresponde ao vetor indexador relacionado aos módulos de amplitude do sinal, B_k corresponde ao vetor indexador chave de valores aleatórios e *mod k* corresponde a operação módulo do número de diferentes módulos de amplitude do sinal.

Fazendo uma comparação do vetor indexador C_k aos diferentes valores de módulo de amplitude do sinal, um vetor real A_{crip} é criado contendo n_s valores de módulo de amplitude.

Por fim, este vetor real de valores de módulo de amplitude é combinado ao vetor real de valores de fase, já criptografados anteriormente, resultando no vetor complexo S_{crip} dado por:

$$S_{crip} = \sum_{j=1}^{n_s} A_{crip} e^{i\theta_{crip}} \tag{5}$$

em que n_s representa o número de fatias do sinal, A_{crip} corresponde ao vetor real de módulos de amplitude relacionados a C_k e θ_{crip} corresponde ao vetor real de valores de fase já criptografados.

Após isso, o vetor complexo S_{crip} contendo o sinal criptografado passa para o módulo de conversão serial para paralelo, conforme a Fig. 7, e continua o processo de modulação OFDM até a sua transmissão por algum canal. Em nossos resultados, que serão apresentados no Capítulo seguinte, utilizamos uma simulação de um canal AWGN para a realização dos testes.

3.2.2. Descriptografia

No receptor, o sinal criptografado recebido passa pelo processo de demodulação OFDM, conforme a Fig. 7, e os valores são armazenados em um vetor complexo. Este vetor é separado em dois vetores reais, contendo os valores de módulo de amplitude e dos valores de fase, respectivamente. De forma semelhante ao que foi feito durante a segunda parte da criptografia, cria-se um vetor real indexador C'_k composto de n_s números inteiros com valores de 0 a *k-1* relacionados aos valores de módulo de amplitude do sinal recebido. Após isso, o vetor real indexador D_K é criado e dado por:

$$D_k = (k + B_k + C'_k) mod\ k \tag{6}$$

no qual k corresponde ao número de diferentes módulos de amplitude do sinal, B_k corresponde ao vetor indexador chave gerado durante a segunda parte da criptografia e C'_k corresponde ao vetor real indexador relacionado ao sinal recebido.

Fazendo uma comparação do vetor indexador D_k aos diferentes valores de módulo de amplitude do sinal, um vetor real A_{dec} é criado contendo n_s valores de módulo de amplitude, que são os valores de módulo de amplitude do sinal descriptografado. Por fim, o vetor complexo S_{dec} é criado e dado por:

$$S_{dec} = \sum_{k=1}^{n} A_{dec} e^{-i\theta_{recebido}\theta_{chave}} \quad (7)$$

no qual *n* corresponde ao número de fatias do sinal recebido, A_{dec} corresponde ao vetor real de módulos de amplitude descriptografado, $\theta_{recebido}$corresponde ao vetor real de ângulos de fase recebidos e θ_{chave} corresponde ao vetor chave de ângulos de fase aleatórios utilizados durante a primeira parte da criptografia. O vetor complexo resultante encontra-se agora descriptografado e pode passar para o processo de desmapeamento dos símbolos complexos em bits.

Finalizada a implementação passamos a fazer simulações para validar a eficácia da criptografia e a performance do sistema como um todo. Os parâmetros utilizados para as simulações e os resultados obtidos com essas simulações serão descritos no capítulo seguinte.

4. Resultados e Discussões

Neste capítulo iremos apresentar os resultados obtidos a partir das simulações numéricas realizadas com o sistema implementado via MATLAB®. Na primeira seção apresentaremos as simulações referentes a modulação DRS-16-QAM. Na segunda seção serão abordados os resultados referentes a modulação 16-QAM Retangular. Por último apresentaremos uma comparação das BER entre as duas modulações utilizadas, com e sem a presença de criptografia, sendo transmitidas por um canal com ruído AWGN e diferentes valores de SNR.

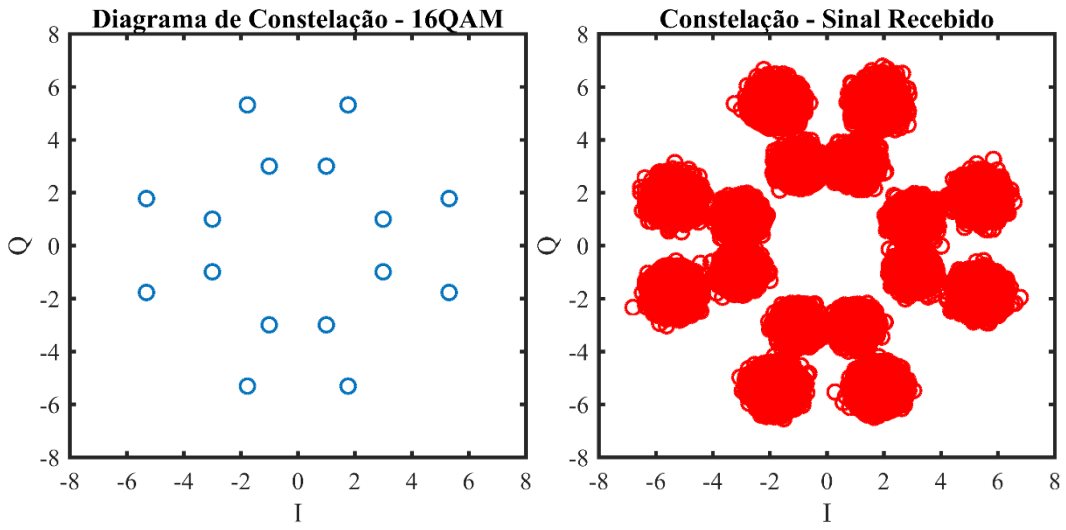
4.1. Parâmetros Utilizados e Resultados Obtidos

Primeiramente fixamos os parâmetros iniciais do modem OFDM com os valores ótimos (que produzem transmissões com menor taxa de erros) para modulações 16-QAM obtidos por meio de [11]. Os valores utilizados podem ser encontrados na Tabela 3. As primeiras simulações que iremos apresentar são da transmissão de um sinal com a modulação DRS-16-QAM. Após iremos apresentar os resultados referentes ao sistema utilizando o a modulação 16-QAM Retangular.

Tabela 3 - Parâmetros utilizados no modem OFDM.

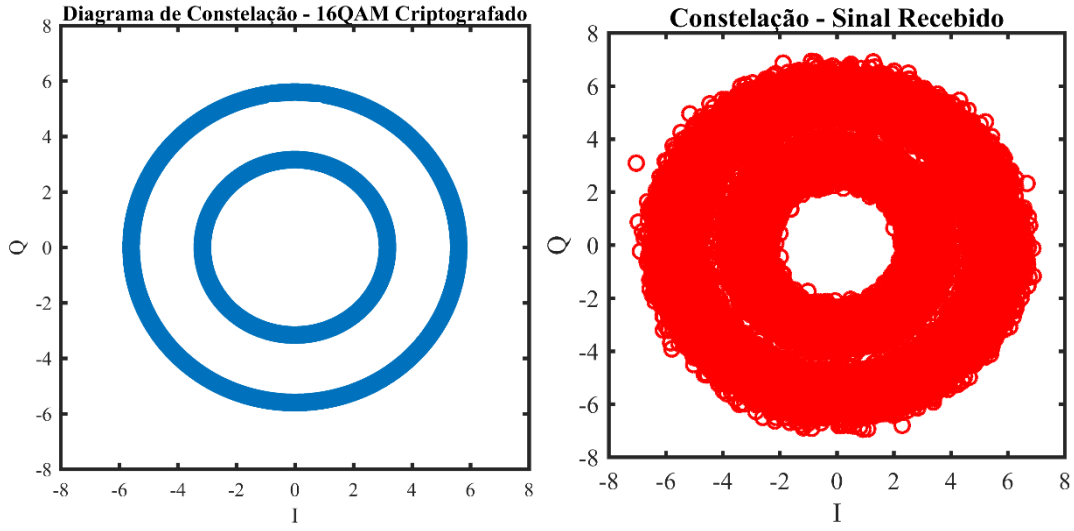
Parâmetros OFDM	
Taxa de bits	1 Gbps
Nº de bits simulados	524016
Nº de amostras	631680
Nº amostras por fatia espectral	1
Frequência de amostragem (GHz)	1.2048
Nº Subportadoras	128
Nº Subportadoras pilotos	20
Prefixo cíclico (%)	10
SNR canal AWGN (dB)	22

4.1.1. Simulação DRS-16-QAM



(a) (b)

Figura 9 - Diagrama de Constelação do sinal de entrada (a) e do sinal recebido sem criptografia (b).



(a) (b)

Figura 10 - Diagrama de Constelação do sinal de entrada criptografado no transmissor (a) e no receptor (b).

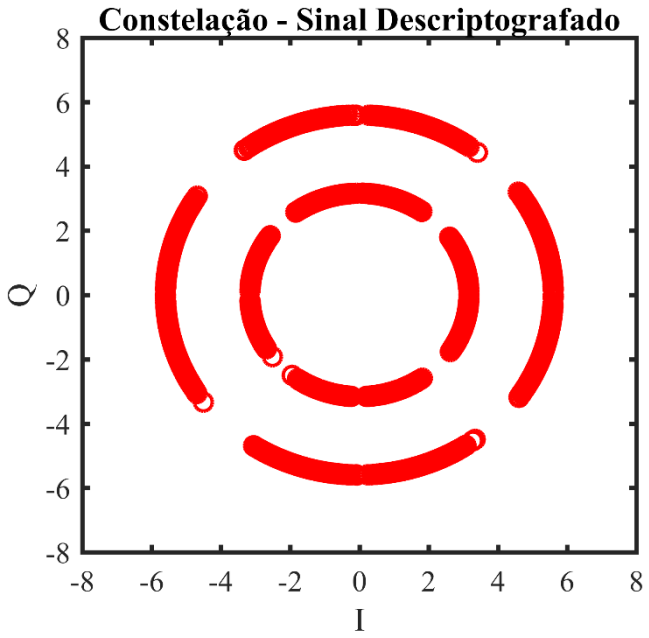


Figura 11 - Constelação do sinal recebido descriptografado.

Na Fig. 9a podemos observar o diagrama de constelação do sinal de entrada, conforme a implementação descrita na seção 2.3.3., e a Fig. 12 nos mostra o histograma referente a este mesmo sinal, com a distribuição de pontos da constelação. Na Fig. 9b, temos o diagrama de constelação deste mesmo sinal no receptor, após passar pelo canal AWGN de SNR = 22 dB, sem a utilização de criptografia. A BER média nesse caso é igual a $1{,}336 \times 10^{-05}$. Após, na Fig 10a podemos observar o diagrama de constelação do sinal de entrada após passar pela criptografia. Em seguida, na Fig 10b, este mesmo sinal recebido no receptor, após passar pelo canal AWGN de SNR = 22 dB, possuindo uma BER = 0,4993. Esta BER é aproximadamente a maior BER que pode ser obtida. O histograma referente a este sinal criptografado pode ser observado na Fig. 13. Assim, os bits após a demodulação possuem uma alta descorrelação com o sinal original, o que nos mostra a robustez da criptografia. Na Fig. 11 observamos o sinal recebido após passar pela descriptografia, a BER média neste caso também é $1{,}336 \times 10^{-05}$. O formato da constelação muda devido ao detector, no entanto, se observarmos na Fig. 14 o histograma deste mesmo sinal, poderemos ver que a maior concentração dos pontos da constelação estão nas amplitudes referentes ao sinal de entrada. A BER média é calculada pela técnica de contagem de erros (*Error Counting*) após realizar cinco simulações com sequências de bits iniciais diferentes e fazer a média das taxas encontradas.

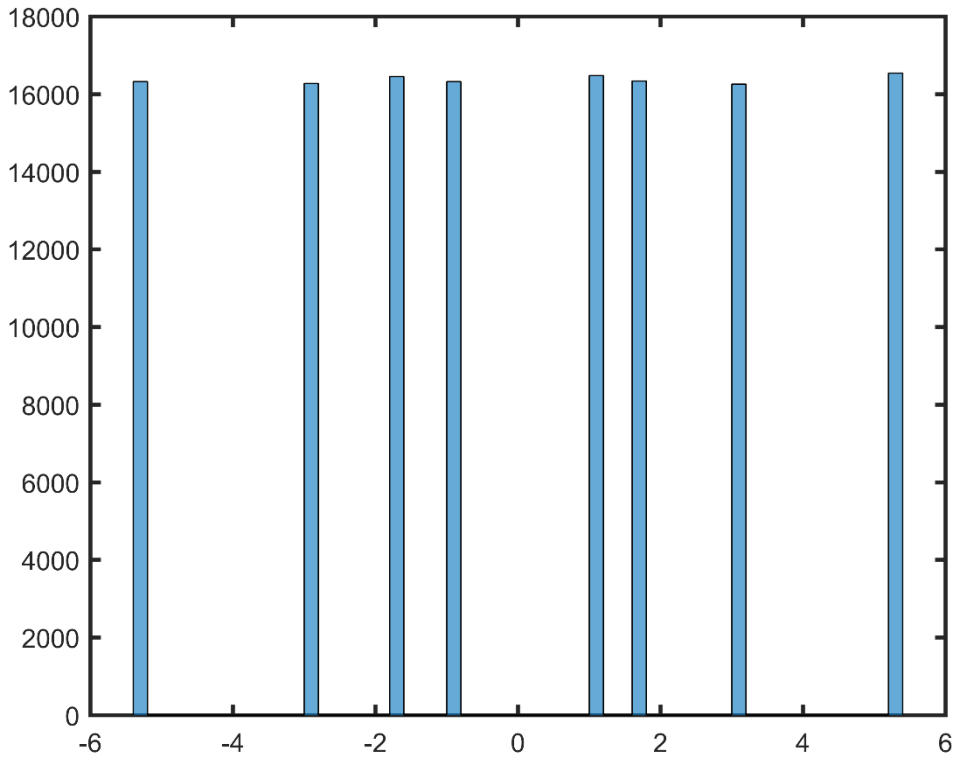


Figura 12 - Histograma da parte real do sinal de entrada antes da criptografia. (DRS-16-QAM)

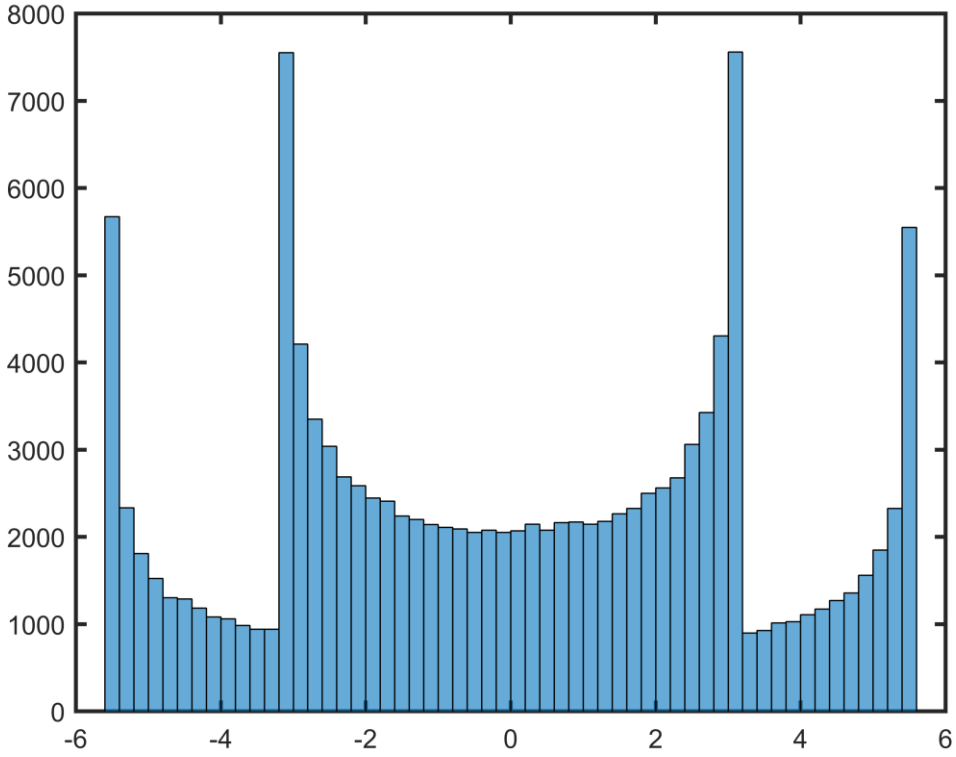


Figura 13 - Histograma da parte real do sinal criptografado (DRS-16-QAM).

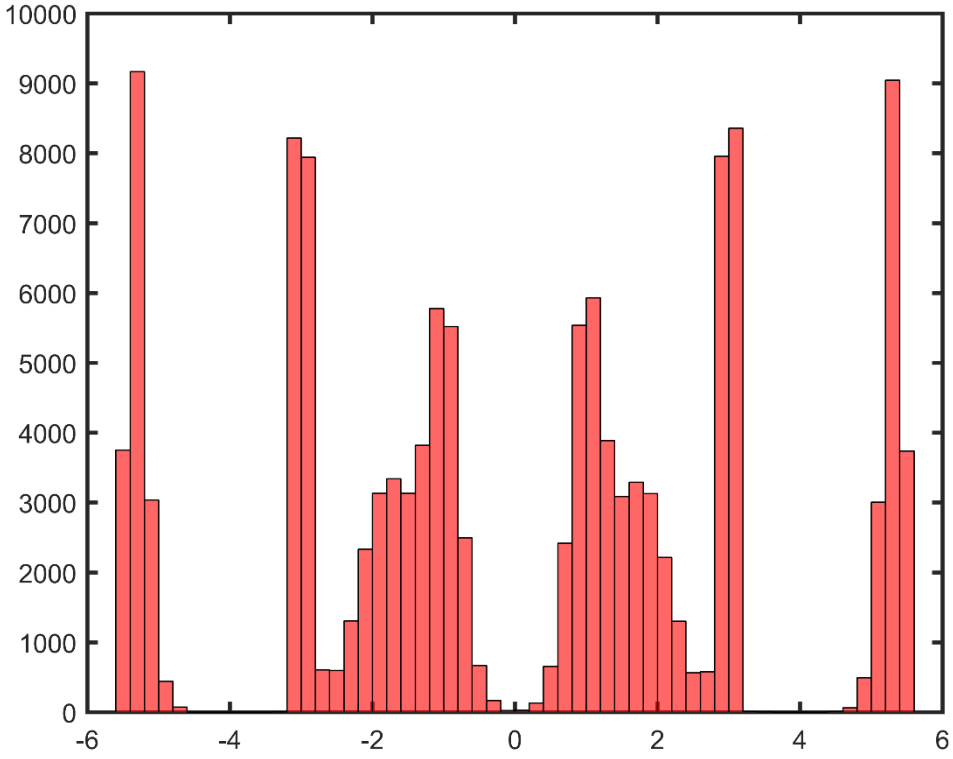
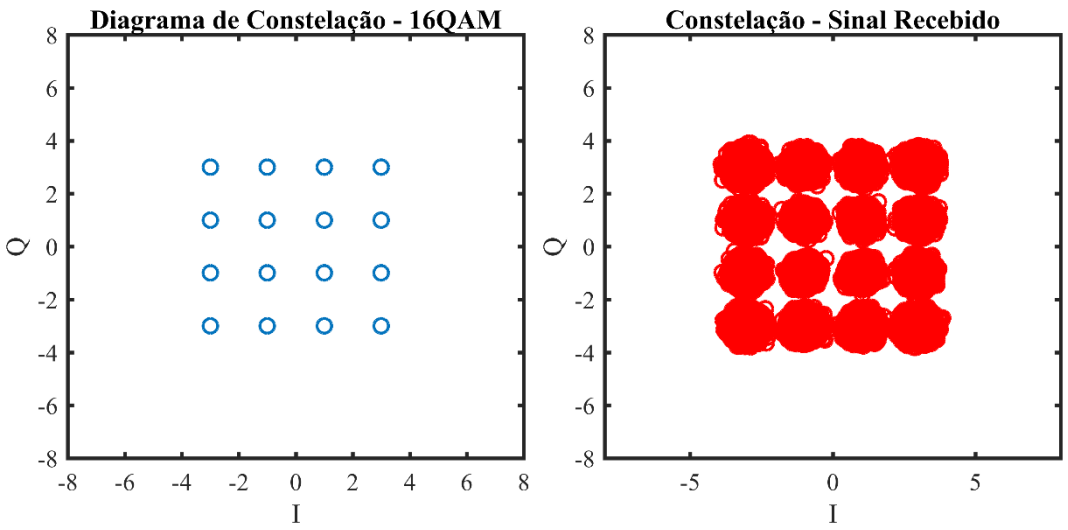


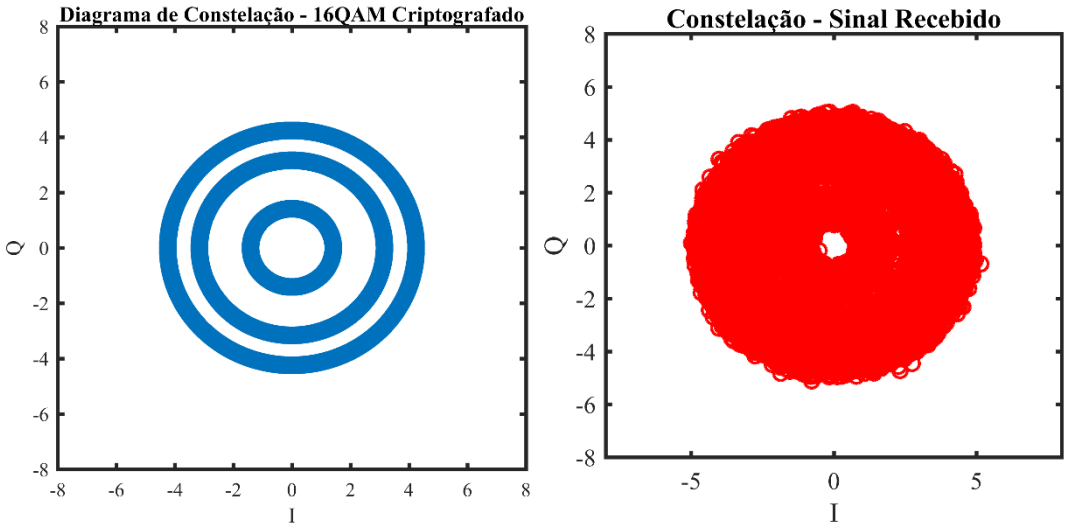
Figura 14 – Histograma da parte real do sinal recebido descriptografado. (DRS-16-QAM)

4.1.2. Simulação 16-QAM Retangular



(a) (b)

Figura 15 - Diagrama de Constelação do sinal de entrada (a) e do sinal recebido sem criptografia (b) (16-QAM Retangular).



(a) (b)

Figura 16 - Diagrama de Constelação do sinal de entrada criptografado no transmissor (a) e no receptor (b) (16-QAM Retangular).

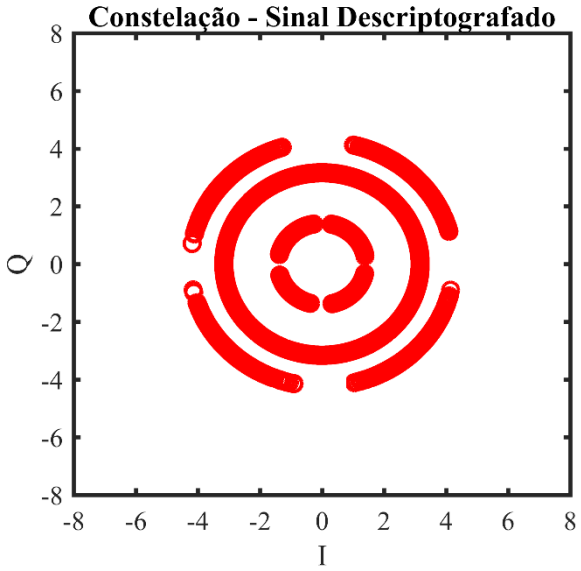


Figura 17 - Constelação do sinal recebido descriptografado (16-QAM Retangular).

Iremos fazer uma análise semelhante ao que foi feito na seção anterior, mas agora referente à modulação 16-QAM Retangular. Na Fig. 15a podemos observar o diagrama de constelação do sinal de entrada, e a Fig. 18 nos mostra o histograma referente a este mesmo sinal, com a distribuição de pontos da constelação. Na Fig. 15b, temos o diagrama de constelação deste mesmo sinal no receptor, após passar pelo canal AWGN de SNR = 22 dB, sem a utilização de criptografia. A BER média nesse caso é igual a 0, pois não existiram erros durante a transmissão. Após, na Fig 16a podemos observar o diagrama de constelação do sinal de entrada após passar pela criptografia. Em seguida, na Fig 16b, este mesmo sinal recebido no receptor, após passar pelo canal AWGN de SNR = 22 dB, possuindo uma BER = 0,5. Esta BER é a maior BER que pode ser obtida. O histograma referente a este sinal criptografado pode ser observado na Fig. 19. Desta maneira, os bits após a demodulação estão totalmente descorrelacionados com o sinal original, semelhantemente ao que foi apresentado para o sinal de modulação DRS-16-QAM, nos mostrando a robustez da criptografia. Na Fig. 17 observamos o sinal recebido após passar pela descriptografia, A BER média é igual a 0.002298, e nos mostra claramente que a implementação da criptografia neste tipo de modulação provoca geração de erros na transmissão. Assim como a modulação DRS-16-QAM, o formato da constelação muda devido ao detector, no entanto, se observarmos na Fig. 20, o histograma deste mesmo sinal, poderemos ver que a maior concentração dos pontos da constelação está nas amplitudes referentes ao sinal de entrada.

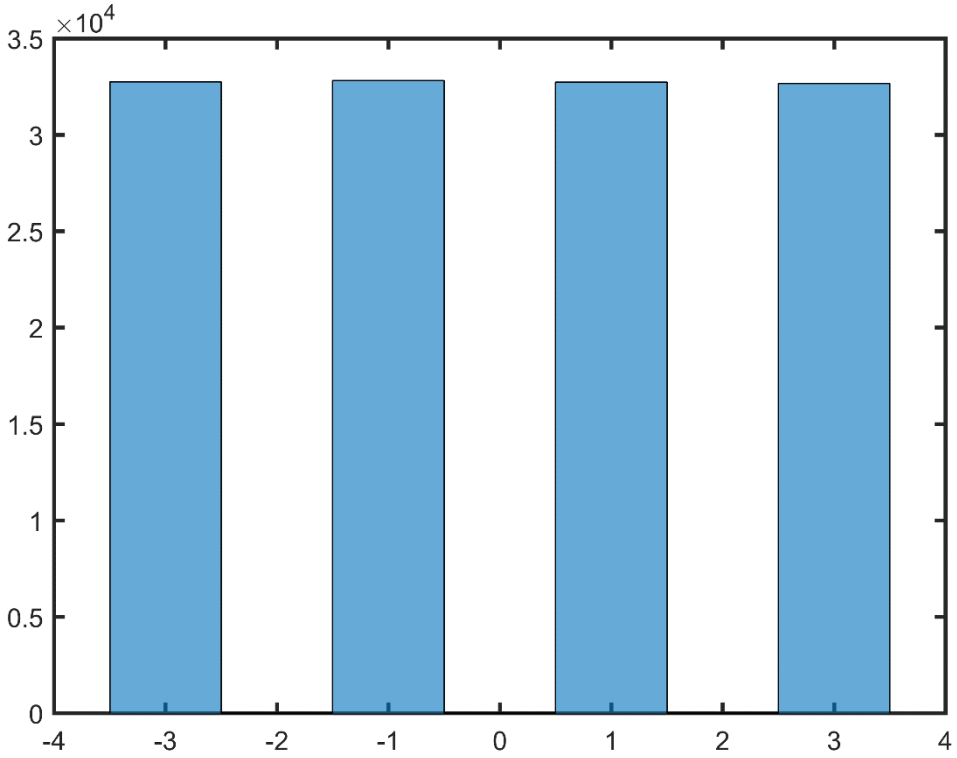


Figura 18 - Histograma da parte real do sinal de entrada antes da criptografia (16-QAM Retangular).

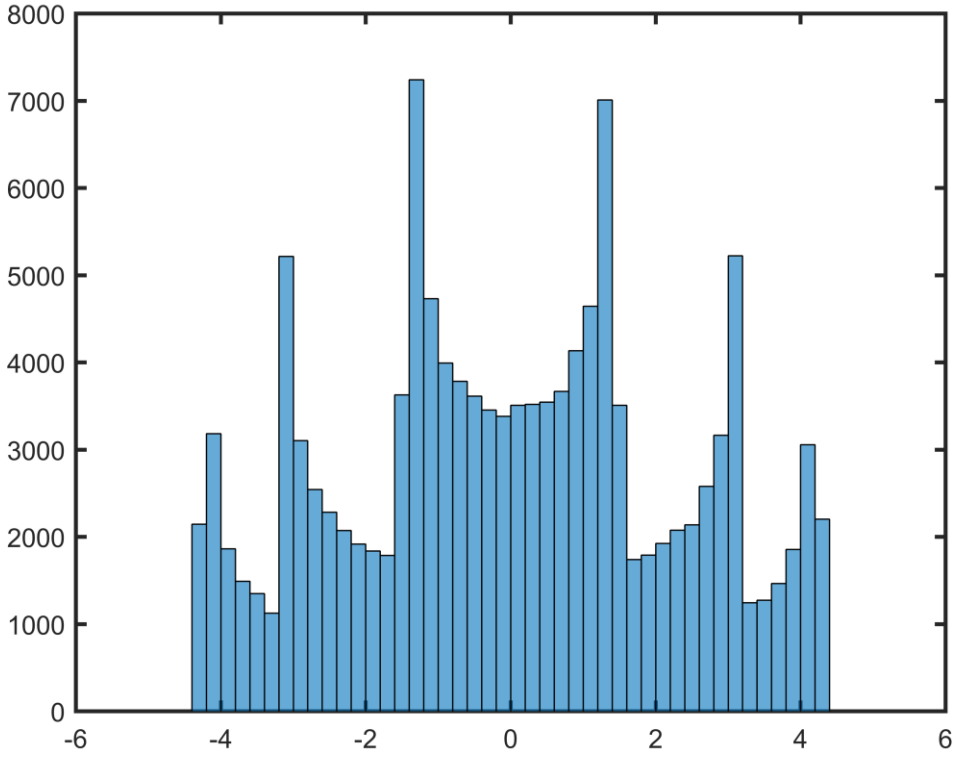


Figura 19 - Histograma da parte real do sinal criptografado (16-QAM Retangular).

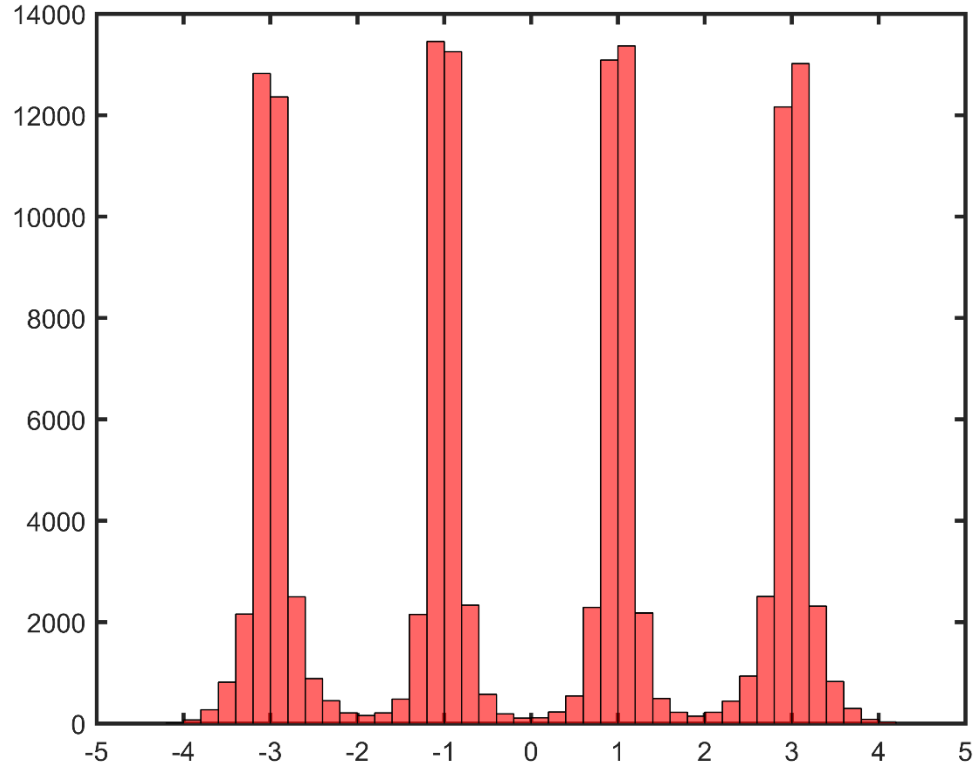


Figura 20 – Histograma da parte real do sinal recebido descriptografado (16-QAM Retangular).

4.2. Comparativo entre os formatos de modulação utilizados

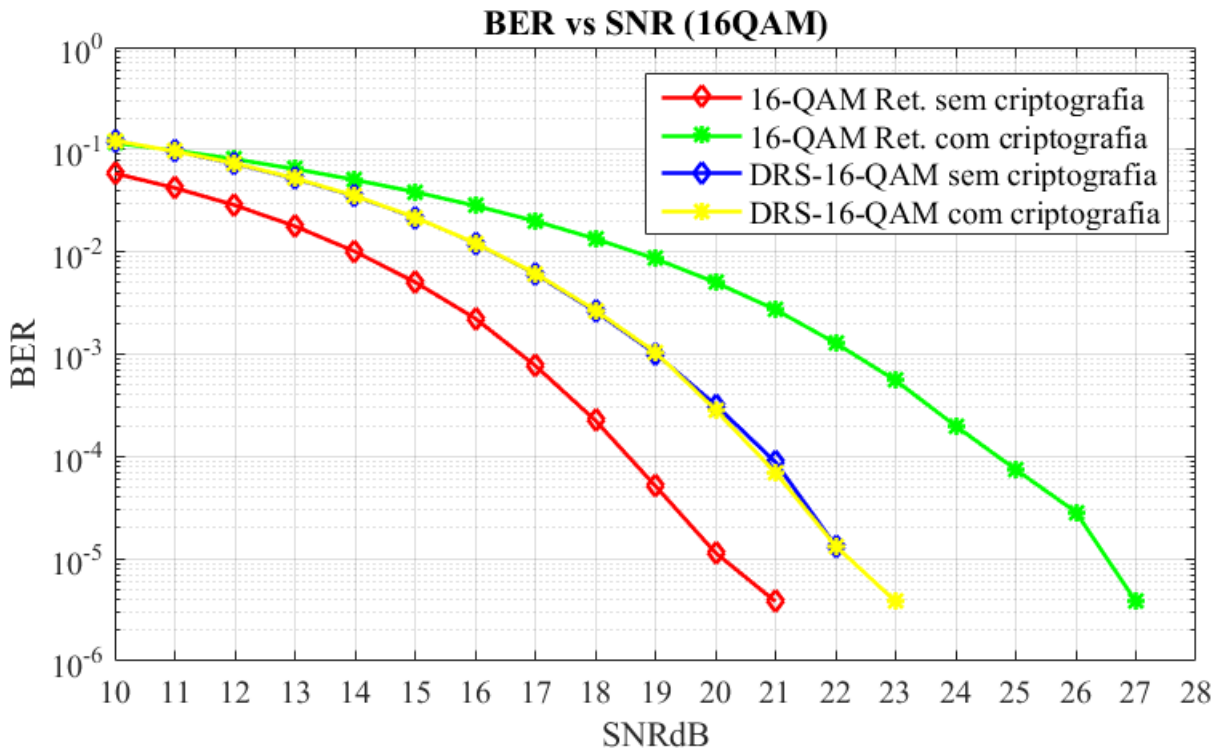


Figura 21 - Diagrama da variação da BER média pela variação da SNR do canal AWGN utilizado durante as transmissões para os diferentes formatos de modulação utilizados.

Durante as simulações foi observado que a BER média para sinais com modulações 16-QAM Retangular era muito superior quando comparado com o sinal sem o uso de criptografia ou com a modulação DRS-16-QAM em um canal de mesma SNR. A Fig. 21 apresenta essa comparação entre as técnicas utilizadas. O que nos mostra que a implementação da criptografia para este formato de modulação 16-QAM traz consigo uma perca de desempenho na transmissão muito alta. Já a modulação DRS-16-QAM se mostrou ótima para este tipo de implementação, pois as diferenças das taxas de erro entre a transmissão do sinal com ou sem a criptografia são mínimas. Um ponto crítico a ser observado é que o sistema oferece BER uma elevada, mas não atende as propriedades criptográficas de Shannon e a segurança semântica pois as chaves se repetem em cada bloco de criptografia. A utilização de chaves dinâmicas é uma possível solução. Outro ponto crítico a ser observado é a não criptografia dos símbolos pilotos, logo um possível intruso pode fazer a estimação do canal através deles. No entanto, não

poderá reconhecer a mensagem. Esses pontos observado são campos abertos para futuras implementações e pesquisas junto a técnica desenvolvida.

5. Conclusões

Neste trabalho de conclusão de curso foi desenvolvida e analisada a implementação de criptografia de sinais baseada em codificação espectral em um sistema de transmissão OFDM utilizando-se de dois tipos diferentes de modulação, a 16-QAM Retangular e a DRS-16-QAM. A técnica de criptografia implementada teve como principal referência a técnica de codificação espectral de fase (SPE), dividindo o sinal transmitido em fatias espectrais e alterando as propriedades das mesmas. Junto a esta técnica, com a proposta de trazer maior robustez a criptografia, foi implementado também uma criptografia das amplitudes de cada fatia. Para a transmissão do sinal, um modulador/demodulador OFDM teórico, desenvolvido em MATLAB® em [11], foi adaptado. A criptografia foi implementada junto ao código, com o módulo de criptografia entrando após o mapeamento dos símbolos no transmissor e, de maneira semelhante, o módulo de descriptografia entrando antes do desmapeamento dos símbolos no receptor.

Após a implementação, foram realizadas simulações com o objetivo de avaliar o desempenho do sistema. Nessas simulações, primeiramente, foi concluído que a técnica de criptografia se mostrou robusta, já que o sinal quando criptografado apresenta uma BER extremamente próximo a BER máxima, o que nos indica alta descorrelação dos bits. Também observamos que utilização da modulação DRS-16-QAM para este tipo de criptografia em transmissões OFDM é mais indicado do que a modulação 16-QAM Retangular, de forma que a primeira apresenta uma taxa de erro menor quando transmitida por um canal AWGN de mesma SNR.

Por fim, observa-se que o presente trabalho é uma ótima contribuição para a comunidade científica pois aborda um tema crucial para os sistemas de transmissão atuais: a segurança e confiabilidade das transmissões. Além disso, o sistema de transmissão OFDM é um dos mais

utilizados atualmente e tem diversas aplicações comerciais e científicas, tanto em transmissões óticas como em transmissões sem-fio.

Devido a pandemia do vírus COVID-19, não foi possível serem feitos testes mais elaborados com este sistema, já que foi necessário o isolamento social. Como uma possibilidade futura, este sistema poderia ser implementado via DSP para a realização de mais testes e futuras publicações.

REFERÊNCIAS

1. KARTALOPOULOS, S. V. A primer on cryptography in communications. **IEEE Communications Magazine**, v. 44, n. 4, p. 146-151, Abr 2006. ISSN 0163-6804.
2. SHANNON, C. E. A Mathematical Theory of Cryptography. **Bell System Technical Journal**, v. 27, n. 3, p. 379-423, 1948.
3. DIFERENÇA entre confusão e difusão. **Funzen**, 2019. Disponivel em: <https://www.funzen.net/po/2019/11/19/diferenca-entre-confusao-e-difusao/>. Acesso em: 28 Out 2020.
4. MOIZUDDIN, M.; WINSTON, J.; QAYYUM, M. A comprehensive survey: Quantum cryptography. **2nd International Conference on Anti-Cyber Crimes (ICACC)**, p. 98–102, 2017.
5. ZHANG, W. et al. Hybrid chaotic confusion and diffusion for physical layer security in ofdm-pon. **IEEE Photonics Journal**, v. 9, n. 2, p. 1-10, 2017.
6. ZHANG, L. et al. Secure OFDM-PON based on chaos scrambling. **IEEE Photon. Technol. Lett**, v. 23, n. 14, p. 998-1000, Jul 2011.
7. SULTAN, A. et al. Dynamic QAM mapping for physical–layer security using digital chaos. **IEEE Access**, v. 6, p. 47199-47205, 2018.
8. CORNEJO, J.; TOCNAYE, J. L. D. B. D. L. Non-invasive WDM channel scrambling for secure high data rate optical transmissions. **In: SHERIDAN, J. T.; WYROWSKI, F. (Ed.). Photon Management III**, v. 6994, p. 124-131, 2008.
9. ABBADE, M. et al. All-optical phase and delay spectral encoding of signals with advanced modulation formats. **International Conference on Transparent Optical Networks**, p. 1-4, Jul 2014. ISSN 10.1109/ICTON.2014.6876372.
10. DE ANDRADE BRAGAGNOLLE, T. et al. All-optical spectral shuffling of signals traveling through different optical routes. **21st International Conference on Transparent Optical Networks (ICTON)**, p. 1-4, 2019.
11. JÚNIOR, A. E. F. **Otimização de subportadoras pilotos em OFDM PONs**. UNESP - Universidade Paulista "Júlio de Mesquita Filho". [S.l.]. 2019.

12. BINH, L. Dual-ring 16-Star QAM direct and coherent detection in 100 Gb/s optically amplified fiber transmission: Simulation. **Optical and Quantum Electronics**, v. 40, p. 707-732, Dez 2008. ISSN 10.1007/s11082-008-9260-3.

13. DOELZ, M. L.; HEALD, E. T.; MARTIN, D. L. **Binary data transmission techniques for linear systems**. Proc. IRE. [S.l.], p. 656–661. Maio 1957. (ISSN 0096-8390).

14. CHANG, R. W. Synthesis of band-limited orthogonal signals for multichannel data transmission. **Bell Syst. Tech. J.**, v. 45, p. 1775–1796, Dezembro 1966.

15. WEINSTEIN, S. B.; EBERT, P. M. Data transmission by frequency-division multiplexing using discrete Fourier transform. **IEEE Transactions on Communication Technology**, v. 19, n. 5, p. 628 - 634, Outubro 1971.

16. PELED, A.; RUIZ, A. Frequency domain data transmission using reduced computational complexity algorithms. **Acoustics, Speech, and Signal Processing**, IEEE International Conference on ICASSP '80, v. 5, p. 964-967, 1980.

17. CIMINI, L. Analysis and Simulation of a Digital Mobile Channel Using Orthogonal Frequency Division Multiplexing. **IEEE Transactions Communications**, p. 665-675, 1985. ISSN 10.1109/TCOM.1985.1096357.

18. PINTO, E. L.; ALBUQUERQUE, C. P. A técnica de transmissão OFDM. **Revista Científica Periódica - Telecomunicações**, v. 5, n. 1, Jun 2002. ISSN 1516-2338.

19. ARNDT, D. M.. F. 2. **Análise comparativa entre os sistemas ofdm e fbmc na transmissão de tv digital**. Universidade Federal de Santa Catarina - UFSC. Florianópolis. 2012.

20. ISLAM, K. M. et al. Performance Comparison between Traditional and Gray-mapped 16-QAM Scheme with OFDM in both AWGN and Rayleigh Fading Channel, Mai 2011.

21. BINH, L. Optical Fiber Communication Systems with MATLAB and Simulink Models. 2º. ed. [S.l.]: CRC Press, 2014. p. 598-602.

22. SEIMETZ, M.; NOELLE, M.; PATZAK, E. Optical systems with high-order DPSK and star QAM modulation based on interferometric direct detection. **IEEE Journal of Lightwave Technology**, v. 25, p. 1515–1530, 2007.

23. YOON, H.; LEE, D.; PARK, N. Performance comparison of optical 8-ary differential phase-shift keying systems with different electrical decision schemes. **Optic Express**, v. 13, p. 371–376, 2005.

24. SANTOS, M. D. O. **Criptografia na camada física baseada em codificação espectral implantada por meio de DSP e aplicada a redes ópticas**. UNESP - Universidade Estadual Paulista "Júlio de Mesquita Filho". São João da Boa Vista. 2020.

25. LIAO, S. et al. Satellite-to-ground quantum key. **Nature 549**, p. 43-47, 2017.