UNIVERSIDADE ESTADUAL PAULISTA “JÚLIO DE MESQUITA FILHO”

CÂMPUS EXPERIMENTAL DE SÃO JOÃO DA BOA VISTA

BACHARELADO EM ENGENHARIA ELETRÔNICA E DE TELECOMUNICAÇÕES

JOÃO PEDRO DE LIMA CASSIANO PEREIRA

ANÁLISE DE DIFUSÃO E CONFUSÃO PARA REDES DE FEISTEL APLICADA À SINAIS

SÃO JOÃO DA BOA VISTA

2020

JOÃO PEDRO DE LIMA CASSIANO PEREIRA

ANÁLISE DE DIFUSÃO E CONFUSÃO PARA REDES DE FEISTEL APLICADA À SINAIS

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

Orientador: Prof. Dr. Marcelo Luís Francisco Abbade

SÃO JOÃO DA BOA VISTA

2020

P436a

Pereira, João Pedro de Lima Cassiano
Análise de difusão e confusão para redes de Feistel aplicadas a sinais / João Pedro de Lima Cassiano Pereira. -- São João da Boa Vista, 2020
37 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

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

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

Essa ficha não pode ser modificada.

UNIVERSIDADE ESTADUAL PAULISTA

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

TRABALHO DE CONCLUSÃO DE CURSO

ANÁLISE DE DIFUSÃO E CONFUSÃO PARA REDES DE FEISTEL APLICADA À SINAIS

Aluno: João Pedro de Lima Cassiano Pereira
Orientador: Prof. Dr. Marcelo Luís Francisco Abbade

Banca Examinadora:

- Marcelo Luís Francisco Abbade (Orientador)
- Ivan Aritz Aldaya Garde (Examinador)
- Rafael Abrantes Penchel (Examinador)

A ata da defesa com as respectivas assinaturas dos membros encontra-se no prontuário do aluno (Expediente nº 30/2019)

São João da Boa Vista, 27 de novembro de 2020

DEDICATÓRIA

Dedico este trabalho aos meus pais, Leandro e Marlene e minha irmã Ana Estela, por todo apoio, incentivo e ajuda para superar todas as dificuldades durante o período de graduação. Aos meus colegas de graduação, André, Felippe, Homero, João Gabriel, José Carlos, José Victor, Luís Antônio, Marcelo, Matheus Galli, Matheus Valério, Ricardo Borges, Ricardo Michelin, Romulo e Silvio, que foram muito importantes no compartilhamento de conhecimento durante todo o curso

AGRADECIMENTOS

Ao meu orientador, Prof. Dr. Marcelo Luís Francisco Abbade, por todo o ensinamento passado por todo período de graduação, paciência e dedicação para que este trabalho fosse concluído.

Ao Thiago de Andrade Bragagnolle pela ajuda e compartilhamento de conhecimento sobre o tema abordado no trabalho.

Aos meus familiares e amigos que sempre me apoiaram durante toda jornada acadêmica, e a todos os professores que tive durante este período.

A todos que contribuíram de maneira direta ou indiretamente para a realização deste trabalho.

“Nunca deixe que lhe digam que não vale a pena acreditar no sonho que se tem ou que os seus planos nunca vão dar certo”

(Renato Russo)

RESUMO

Com o crescente aumento do uso de dados no nosso cotidiano, cada vez mais os dados se tornam importantes e sensíveis. Dados podem conter informações pessoais ou sigilosas, que podem comprometer nossa privacidade. Diante disso, criminosos estão cada vez mais motivados a obter dados de terceiros. Os métodos criptográficos tem como objetivo dificultar esse acesso indevido aos dados, onde somente o transmissor e o receptor interpretem as mensagens entre eles. Muitas técnicas criptográficas são aplicadas à dados, encriptando a mensagem nas 6 camadas superiores do modelo OSI. Neste trabalho foi estudado um método criptográfico onde a encriptação ocorre nos sinais, ou seja, na camada física do modelo OSI. Este trabalho consiste em estudar o uso de uma rede Feistel aplicada a sinais, levando a sinais criptografados com uma taxa de erro de bits de aproximadamente 50% que satisfazem os requisitos de difusão criptográfica e confusão.

Palavras-chave: Segurança, criptografia, cifra de blocos, criptografia de sinais, rede de Feistel

ABSTRACT

With the increasing use of data in our daily lives, more and more data becomes important and sensitive. The data may contain personal or confidential information, which may compromise our privacy. Given this, criminals are increasingly motivated to obtain data from third parties. Cryptographic methods aim to hinder this improper access to data, where only the transmitter and receiver interpret it as messages between them. Many cryptographic techniques are applied to data, encrypting the message in the top 6 layers of the OSI model. In this work, a cryptographic method was studied where encryption occurs in signals, that is, in the physical layer of the OSI model. This work consists of studying the use of a Feistel network applied to signals, leading to encrypted signals with a bit error ratio of ~50% that satisfy the requirements of cryptographic diffusion and confusion.

Keywords: Security, encryption, block cipher, signal encryption, Feistel network

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE SIGLAS E ABREVIATURAS

BER	Bit Error Ratio
DES	Data Encryption Standard
FPGA	Field-Programmable Gate Array
ISO	International Organization for Standardization
OSI	Open System Interconnection
QPSK	Quadrature Phase Shift Keying
RAD	Radianos
USRP	Universal Software Radio Peripheral
XOR	Exclusive or

SUMÁRIO

1 – Introdução

Neste capítulo serão abordados os conceitos necessários para a compreensão do trabalho realizado. Na Seção 1.1 apresenta-se a motivação de utilizar criptografia, e exemplifica-se o funcionamento de uma criptografia simples e de uma cifra de blocos. Na Seção 1.2 é descrito as métricas para avaliar o desempenho de um método de encriptação. Na Seção 1.3 é discutido a diferença entre uma criptografia de dados e uma criptografia de sinais, e a maneira que uma criptografia de sinais é realizada. Posteriormente na seção 1.4 é mostrado as contribuições geradas por este trabalho, já na seção 1.5 é apresentada a maneira que o trabalho foi estruturado.

1.1 – Criptografia

Atualmente os dados são um dos bens mais valiosos do mundo, conforme dito pelo CEO da Mastercard Ajay Banga, os dados são o novo petróleo [Julio, 2019]. De fato os dados se tornaram parte dos nossos "bens" e há uma grande preocupação em protege-los. Pelo motivo que alguns deles contém informações sigilosas, que podem expor informações privadas do proprietário dos dados. Como as informações trafegam por meios públicos, por exemplo, um sinal de rádio que se propaga pelo ar pode ser captado por um invasor com o uso de uma antena. Apesar de alguém não autorizado poder captar a informação, a solução encontrada para a proteção dos dados é, que a pessoa não autorizada não possa compreender o significado da informação. Com isso, houve a implantação da criptografia.

A palavra criptografia tem como origem duas palavras gregas, *Kryptos* (Oculto) e *Gráphein* (Escrita). A junção de ambas oferece o significado de ocultar o que está escrito. Para este trabalho, o estudo considerado sobre criptografia está relacionado com um dos pilares da segurança da informação, a confidencialidade, conforme descrito em [Stallings, 2014]. Este pilar pode ser exemplificado por assegurar que somente os proprietários dos dados tenham acesso aos mesmos.

Em uma transmissão de dados, temos que esse pilar é garantido somente quando o transmissor e o receptor são os únicos a ter acesso aos dados. Um exemplo simples de criptografia para exemplificar o tema é a cifra de César, apresentada em [Terrada, 2008]. A cifra consiste em utilizar uma tabela que faz correspondência de um texto original com um texto de uma mensagem cifrada. Se hipoteticamente desejamos encriptar a palavra

UNESP, é possível utilizar uma tabela como a apresentada na figura 1. A tabela da figura vai ser utilizada como uma regra de conversão, em que cada letra da primeira linha será trocada pela sua respectiva letra da terceira linha.

Letras alfabeto convencional	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
Letras do código cifrado	C	N	A	V	M	O	B	Z	L	K	P	E	J	Q	D	G	T	X	F	Y	W	R	H	U	I	S

Figura 1 – Troca de letras da Cifra de César

No caso, as letras da palavra UNESP seriam substituídas pelas letras WQMFG, de acordo com a tabela apresentada na figura 1. Ao enviar essa mensagem, em princípio, um interceptador não compreenderá o conteúdo da mensagem sem o uso de ataques criptográficos.

Existem dois métodos de encriptação: cifras de fluxo e cifras de blocos. Segundo [Stallings, 2014] o método de cifra de fluxo encripta apenas um bit por vez da mensagem. Já o método de cifra de blocos, como mostrado em [Burnett, 2002], requer que o texto seja divido em blocos de bits e cada um deles é encriptado individualmente. Para recuperar a mensagem será necessário aplicar a chave novamente a cada bloco, uni-los para ler a mensagem como era antes da codificação. Um exemplo dessa técnica seria: ao encriptar uma mensagem de 256 bits, podemos dividi-la em quatro blocos de 64 bits. Cada bloco passará individualmente por uma operação criptográfica, conforme mostrado na Figura 2. As cifras de fluxo são usadas normalmente para transmitir as chaves que serão utilizadas para criptografar as cifras de bloco. Conforme mostrado em [Katz, 2015], existem dois tipos mais utilizados de cifra de blocos: I) Redes de permutação e substituição e II) Redes de Feistel. As redes de Feistel são o objeto de estudo deste trabalho e estarão explicadas no Capítulo 2.

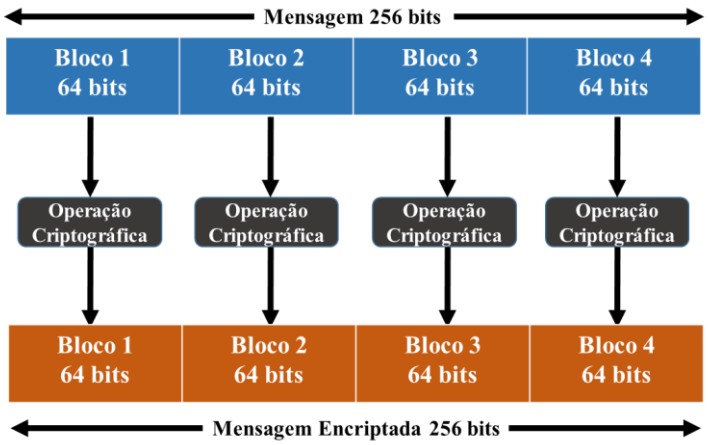

Figura 2 – Operação de Cifra de blocos

1.2 – Métricas de desempenho criptográfico

Há algumas métricas que são utilizadas para avaliar o desempenho de uma cifra criptográfica, entre essas métricas destacam-se a difusão e confusão definidas em [Shannon, 1949]. Ambas são realizadas com o intuito de que alguém que conheça uma parte da mensagem cifrada não consiga realizar a desencriptação. Por exemplo, ao enviar uma mensagem cifrada com dados parecidos para diferentes receptores, alguém que conheça uma das mensagens não deve ser capaz de descobrir as outras analisando o texto cifrado.

A difusão é a propriedade que estabelece que mensagens originais próximas devem ter mensagens cifradas bastante diferentes entre si. Mesmo ao variar-se apenas um bit de uma mensagem original para outra, os textos cifrados correspondentes devem sofrer uma grande alteração. Pode-se considerar que a difusão ocorre de maneira bem sucedida quando a alteração de apenas um bit do texto original implica uma alteração de aproximadamente 50% do texto.

No caso da confusão, a análise consiste na influência da chave criptográfica no texto cifrado. Assim a propriedade define que chaves criptográficas próximas devem ter texto cifrados diferentes para uma mesma mensagem original. Semelhante à difusão, mas alterando a chave, a mudança de um bit na chave deve gerar um texto cifrado com grandes alterações. Considera-se uma confusão bem sucedida quando a alteração no texto cifrado é aproximadamente 50%.

1.3– Criptografia de dados e criptografia de sinais

Conforme descrito em [Tanembaum, 2013], o modelo OSI é o modelo de referência dos protocolos, divididos em camadas de comunicação, este modelo foi elaborado pela ISO. A criptografia de dados atua nas seis camadas superiores do modelo OSI porque essas camadas atuam com valores binários, ou seja, a criptografia de sinais atua em codificar os bits de uma mensagem.

Já na camada física, que converte bits para sinais, é realizado a criptografia de sinais. A criptografia de sinais ocorre diretamente no tipo de sinal que a mensagem está sendo transmitida, seja ele óptico ou de radiofrequência, conforme descrito em [Abbade, 2018]. Assim como a criptografia de dados, a criptografia de sinais altera o sinal de maneira reversível antes de sua transmissão.

Segundo [Breed, 2003] a BER é uma métrica utilizada para avaliar o desempenho de transmissões, ela é a razão entre o número de erros de bits com o total de bits transmitidos. Para uma transmissão espera-se que a BER tenha o menor valor possível, significando que houve um baixo índice de bits errados na recepção. Para a avaliação de um algoritmo criptográfico deseja-se que a BER tenha o maior valor possível de 0,5, significando que após a encriptação metades dos bits foram trocados. Um número grande de bits trocados, demonstra que durante o processo de encriptação a mensagem cifrada não possui semelhança com a mensagem original.

1.4 – Contribuições

Este trabalho contribui com os seguintes aspectos. Inicialmente, apresenta-se um resultado sobre a variação do valor da BER durante uma operação criptográfica de uma rede de Feistel aplicada à sinais. Há também neste trabalho uma análise de confusão e difusão, o qual vai apresentar resultados que permitem avaliar o desempenho criptográfico da rede de Feistel aplicada à sinais. A proposta utilizada no trabalho provém dos trabalhos [Bragagnolle, 2018] e [Souza, 2019].

1.5 –Estrutura do trabalho

O trabalho está organizado da seguinte forma: No Capítulo 2 aborda-se o funcionamento de uma rede de Feistel. A Seção 2.1 apresenta o funcionamento originalmente concebido para a rede de Feistel, a qual é aplicada à dados. Também é discutido nesta seção sobre as vantagens da rede de Feistel possuir circuitos de encriptação e desencriptação semelhantes, além de possuir reversibilidade. Na Seção 2.2 é mostrada a rede de Feistel utilizada para o estudo neste trabalho, a rede de Feistel aplicada à dados. É apresentado como é o funcionamento e como são realizadas as operações da rede de Feistel proposta, onde ao invés de variáveis lógicas serão utilizados variáveis referentes a um sinal.

No capítulo 3 são apresentados os resultados obtidos por meio de simulação durante este trabalho. A seção 3.1 aborda a maneira que foi implantada a rede de Feistel utilizada no trabalho e como foi definida suas funções criptográficas. É abordada a maneira como as chaves são utilizadas e como uma operação lógica foi substituída por uma operação com sinais. Na seção 3.2 é apresentada a análise da BER para a rede de Feistel estudada. Posteriormente na seção 3.3 é realizada uma análise da difusão da rede

de Feistel aplicada à sinais. A análise é feita com auxílio dos histogramas obtidos por meio de simulação, definindo qual a condição para apresentar um bom desempenho de difusão. A seção 3.4 é similar a seção 3.3, mas toda a análise é feita para a confusão. Foi abordada como foi a implementação de uma análise de confusão para uma chave que não é caracterizada inicialmente por bits. O capitulo 4 apresenta as conclusões finais sobre a realização deste trabalho.

2 - Rede de Feistel

Neste capitulo será abordada a descrição do funcionamento de uma cifra de Feistel, e algumas de suas características. Na seção 2.1 será repetida a rede de Feistel aplicada a criptografia dados. Essa é a concepção original para este tipo de rede. Na seção 2.2 será abordada a metodologia proposta em utilizar a rede de Feistel aplicada a sinais.

2.1 – Rede de Feistel aplicada a criptografia de dados

A rede de Feistel é um estrutura de cifra de blocos, utilizada em importantes padrões de segurança, como o *Data Encryption Standard* (DES). Conforme descrito em [Katz, 2015], normalmente o bloco da mensagem a ser criptografada é dividido em duas partes de mesmo tamanho, L_0 e R_0, referentes aos lados esquerdo e direito do bloco respectivamente.

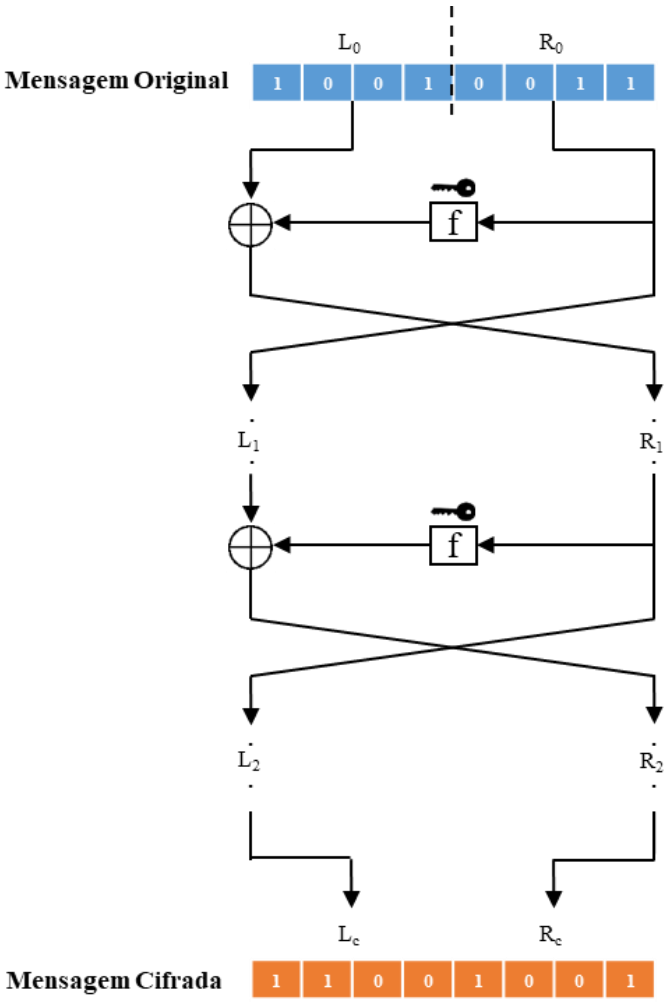

Figura 3 – Rede de Feistel

As metades são submetidas a diferentes processos durante a codificação, como mostrado na Figura 3. Na primeira parte, a metade R_0 é submetida a uma função criptográfica com uma chave. Posteriormente, o resultado é submetido a uma operação XOR com a metade L_0. No final dessa etapa os lados do bloco resultante são invertidos, o resultado da operação com L_0 se torna R_1 e R_0 se torna o L_1. Ao final desse processo com a inversão, temos o que denominamos de ciclo. Também é possível descrever o resultado do ciclo, definindo os valores de L_1 e R_1.

$$L_1 = R_0 \tag{1}$$

$$R_1 = f(R_0) \oplus L_0 \tag{2}$$

No próximo ciclo, a operação é repetida de maneira semelhante ao ciclo anterior, mas utilizando L_1 e R_1. Ao final de dois ciclos temos o que denominamos de rodada, que é caracterizada pelas metades passarem pelo mesmo número de operações. Os ciclos podem ser repetidos tantas vezes quanto necessário. Ao final de todos os ciclos, os dois blocos resultantes são concatenados. Independentemente do número de rodadas, uma mensagem cifrada tem o mesmo tamanho da mensagem original. Equacionando o processo das metades de cada bloco na entrada de um ciclo, é possível obter valores gerais para L e R. Em termos de um valor n para o número do ciclo atual, os valores são dados por:

$$L_n = R_{n-1} \tag{3}$$

$$R_n = f(R_{n-1}) \oplus L_{n-1} \tag{4}$$

Conforme [Stallings, 2014], o circuito de desencriptação de uma rede de Feistel é semelhante ao de encriptação. A reversibilidade da mensagem cifrada é feita com o mesmo circuito da encriptação, invertendo as posições de entrada e saída. Pelo motivo citado, é necessário conhecer o número de ciclos utilizados na encriptação e a chave utilizada com a função criptográfica. A entrada do circuito de desencriptação será o bloco encriptado dividido em L_n e R_n, para um número n de ciclos utilizados na encriptação. Repetindo os ciclos para um valor n, é possível recuperar o sinal criptografado. O valor de n é um número inteiro variando de 1 a N, em que N é o número total de ciclos.

$$L_{n-1} = R_n \oplus f(L_n) \tag{5}$$

$$R_{n-1} = L_n \tag{6}$$

Alguns fatores podem contribuir para uma maior robustez criptográfica da cifra, são eles: tamanho do bloco a ser criptografado, tamanho da chave, número de rodadas, algoritmo de geração da chave e a função criptográfica. Essa robustez é quantificada pela capacidade de difusão e confusão que a cifra implementa, dificultando a interceptação da mensagem.

Outra vantagem da cifra de Feistel, é que devido à sua estrutura, o processo de cifragem é inversivel. Isso ocorre porque cada ciclo pode ser anulado no circuito de decriptação, com a replicação de um ciclo semelhante, conforme descrito em [Feistel, 1975]. Assim, é possível garantir que qualquer operação feita pela função criptográfica *F* pode ser inversivel. Essa vantagem garante que não existirá um caso de uso em que, devido a função *F* utilizada, a mensagem será desencriptada de maneira errada.

2.2 – Rede de Feistel aplicada a criptografia de sinais

O método utilizado para estudo neste trabalho utiliza a rede de Feistel, mas de maneira diferente que citado anteriormente. No caso utilizado para este trabalho, conforme descrito em [Bragagnolle, 2020], o que será encriptado não são os bits da mensagem. No método que é considerado, o bloco de bits é convertido para a camada física em um sinal discreto. Esse sinal é caracterizado por amplitudes e fases, o que será encriptado no método serão as fases.

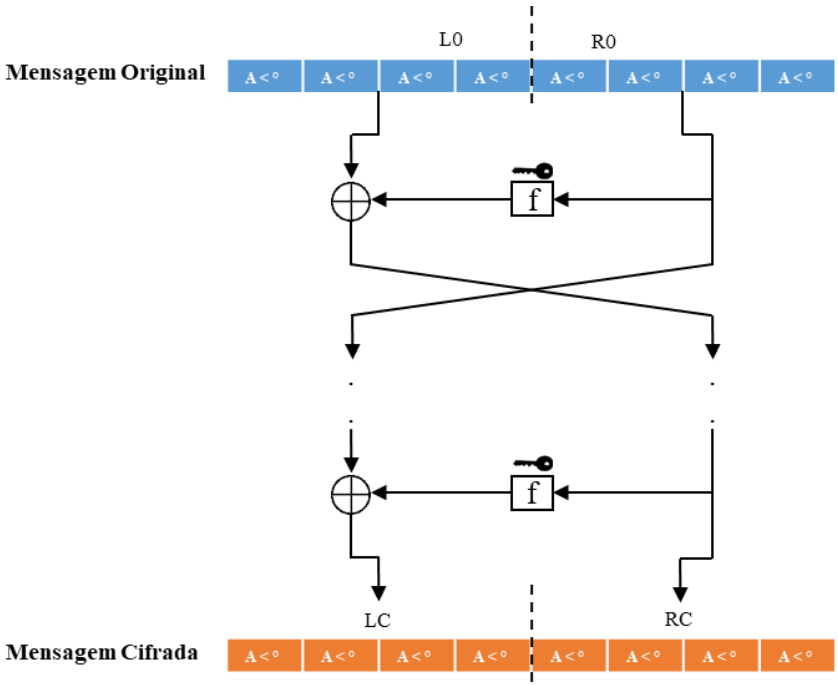

Figura 4 – Rede de Feistel utilizada na técnica

A Figura 4 indica que o bloco constituido por amostra de fases de um sinal discreto também é dividio em duas partes, em um processo semelhante ao mostrado na seção 2.1. No processo, a operação realizada com uma soma de fases entre a metade L_0 e o resultante da função criptográfica com a chave. Portanto, os ciclos seguem a equação (3) como o modelo original da rede, já a equação (4) é modificada, trocando a operação XOR por uma soma de fases.

2.3 – Considerações

Durante esse capítulo foram abordados o funcionamento da rede de Feistel, suas principais características e como a rede foi implantada na encriptação de sinais. A motivação pelo estudo do funcionamento da rede, aconteceu devido a mesma compor um dos dois tipos de cifra de blocos. É importante destacar o fato da rede apresentar confusão, difusão, inversibilidade e um circuito de desencriptação similar ao de encriptação.

3 – Resultados e discussões

Na seção 2.2 abordou-se a aplicação da rede de Feistel aplicada à sinais. Neste capítulo serão descritos os resultados encontrados durante a execução do trabalho. Os resultados foram obtidos a partir de simulações realizadas com códigos criados no *Software* Matlab. A partir desse código realizou-se a codificação e a decodificação de sinais transmitidos por redes de Feistel. Também foi implementado a geração de blocos e chaves de maneira aleatória, permitindo uma variação dos mesmos na repetição das simulações.

Na Seção 3.1 será apresentada como foi implantada a rede de Feistel para o caso estudado neste trabalho. A Seção 3.2 apresentará a análise da BER após a encriptação e desencriptação do sinal. Os resultados obtidos para o desempenho de difusão e confusão do sinal encriptado serão apresentados nas Seções 3.3 e 3.4, respectivamente.

3.1 – Rede de Feistel utilizada

A Figura 5 ilustra um diagrama de blocos para um rodada da rede de Feistel utilizada para esse trabalho. Na realização do trabalho foi definida uma função criptográfica *F*, adotando o uso de duas chaves para cada ciclo. Outro ponto idealizado foi que o próximo ciclo utilizaria um par de chaves diferente do ciclo anterior.

Com a posse das chaves definiu-se como será feita a operação entre as chaves e o bloco na entrada da função. Exemplificando para a primeira rodada, no primeiro ciclo serão utilizadas as chaves K_0 e K_1. A operação será feita conforme a Figura 6(a), onde a metade R_0 será duplicada para realizar a operação *F* com as duas chaves em paralelo. Antes da operação com a chave K_0, o vetor de valores R_0 passará por um deslocamento vetorial cíclico de quatro posições para a esquerda. Posteriormente, o deslocamento de posições, o vetor passará por uma operação de soma de fases com a chave k_0. Na outra ramificação o processo é semelhante, mas o deslocamento será de cinco posições para a direita e a chave utilizada será a K_1. No ciclo seguinte como mostrado na Figura 6(b), o processo todo será repetido com as chaves K_2 e K_3

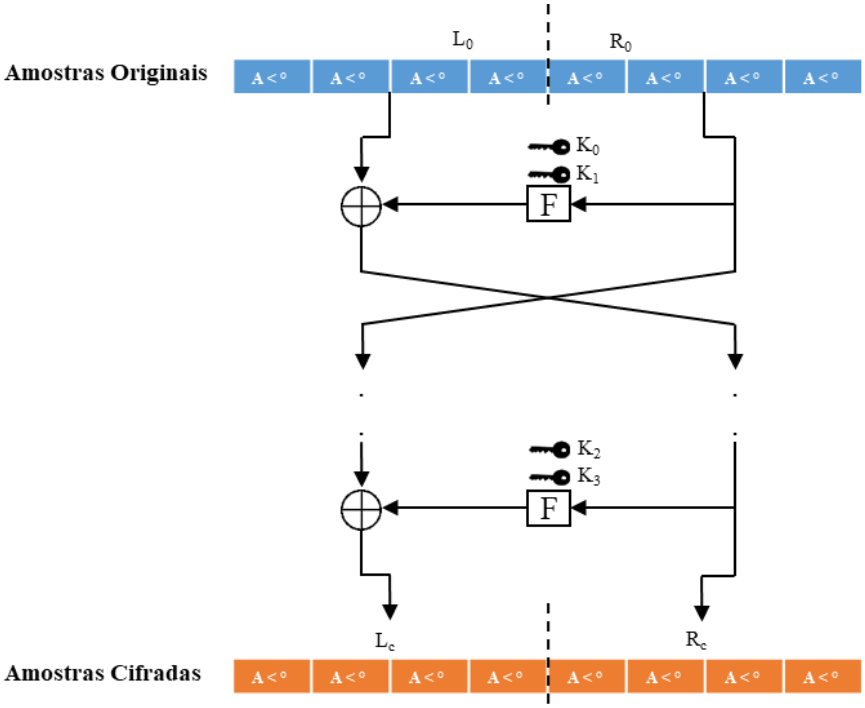

Figura 5 – Diagrama de Blocos para a rede de Feistel utilizada

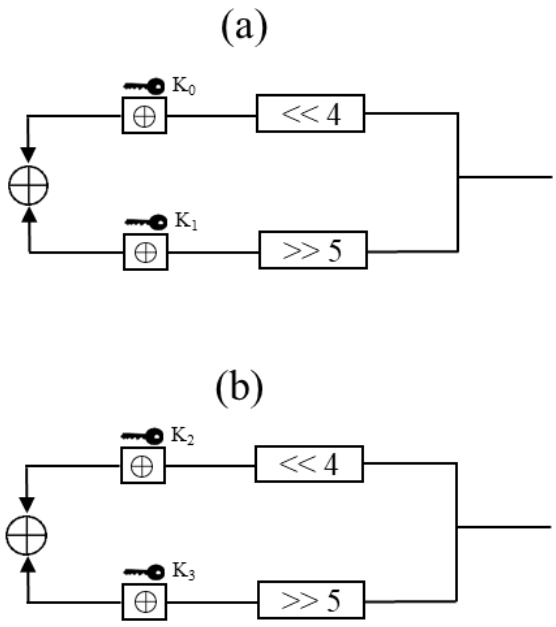

Figura 6 – Função criptográfica utilizada

Ao completar uma rodada, a rodada seguinte utilizará as mesma chaves da anterior. Por isso, como temos dois ciclos em uma rodada, e cada ciclo utiliza duas chaves, totalizando em todo o processo um total de quatro chaves criptográficas.

3.2 – Análise da BER

Durante o trabalho foi feita a análise da BER do sinal após passar pela rede de Feistel com aproximadamente 4640 bits, o número de rodadas foi variado de 1 a 10 e calculada a BER para cada um. Pelo gráfico apresentado pela Figura 7, temos os valores de BER para diferentes números de rodadas.

A construção do gráfico foi feita executando todo o processo da rede de Feistel, repetindo o mesmo para cada valor de rodada. Para a análise foi utilizada uma mensagem de 116 bits em um sinal equivalente complexo em banda base QPSK. Na Figura 7, a variável *n* é o número de rodadas, observamos que a BER não tem uma mudança significativa.

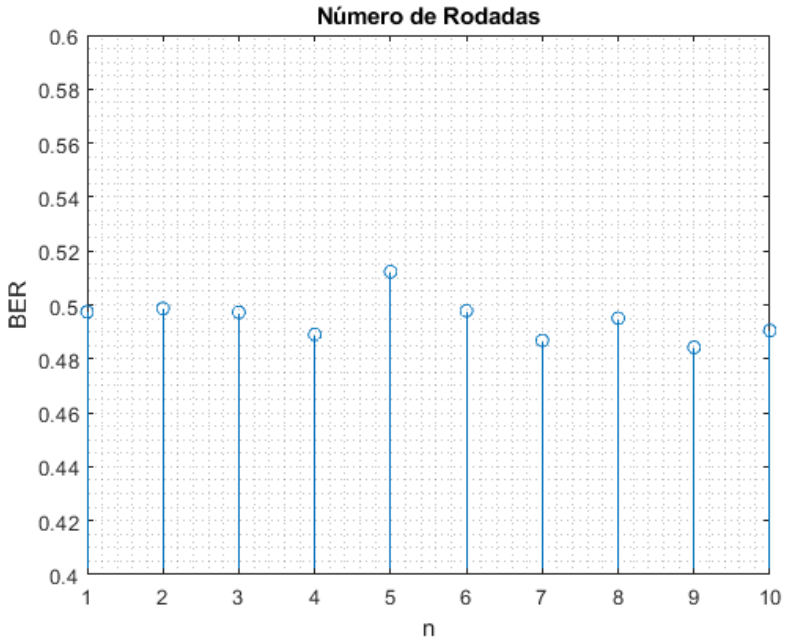

Figura 7 – BER dos sinais encriptados

O desempenho da rede de Feistel aplicada à sinais pode ser avaliada também pelas constelações apresentadas nas Figuras 8, 9 e 10. Na Figura 8 mostramos a constelação do sinal antes de ser encriptado, notamos que as quatro posições da constelação são pontos pequenos e estão distantes, conforme um QPSK. Após a encriptação, como mostrado na Figura 9, observamos vários pontos espalhados e sem padrão de distância entre eles pela constelação. Os pontos espalhados mostram o sucesso do processo de encriptação, pois temos um sinal completamente diferente da mensagem original. A Figura 10 mostra a constelação após a desencriptação, e como ela é idêntica à constelação de encriptação, podemos deduzir que o processo de desencriptação foi bem sucedido, apresentando uma BER resultante nula.

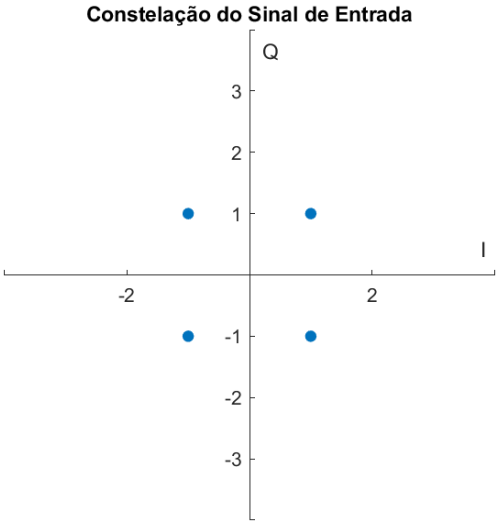

Figura 8 – Constelação do Sinal antes de encriptação

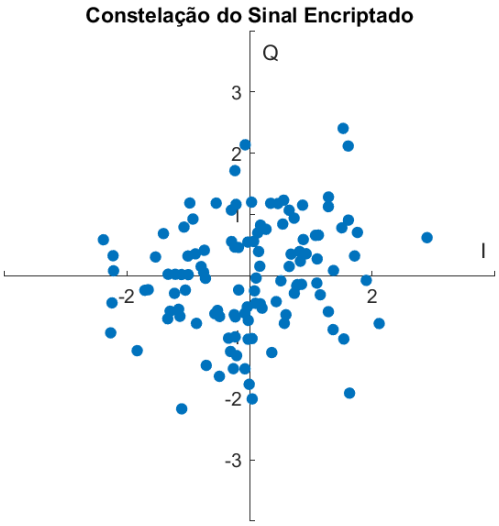

Figura 9 – Constelação do sinal encriptado

Figura 10 – Constelação do sinal desencriptado

3.3 - Análise da Difusão

Para avaliar a difusão provida pela rede de Feistel no estudo, foi utilizada uma amostra com 11.600 bits e repetida para 10 rodadas. Nesse procedimento escolheu-se uma palavra de referência que foi transmitida com uma chave, gerando uma mensagem cifrada de referência. A seguir variou-se o primeiro bit da mensagem de referência, e obteve seu novo texto cifrado. O novo texto cifrado foi comparado com o texto cifrado de referência. O processo de troca de bit do texto de referência foi repetido para todas as posições possíveis de bits da mensagem. A comparação o texto cifrado referente e o texto cifrado de referência nos dá um certo número diferente de bits que pode ser expresso de maneira percentual. Os histogramas das Figuras 11 a 20 mostram uma distribuição desse número de bits alterado em valores percentuais para diferentes números de rodadas da rede de Feistel.

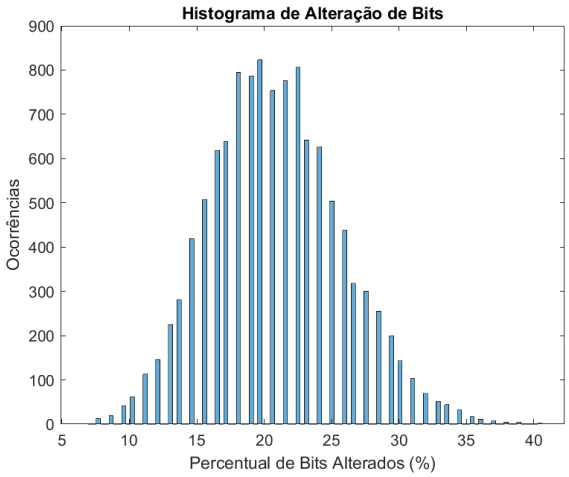

Figura 11 – Histograma para 1 rodada

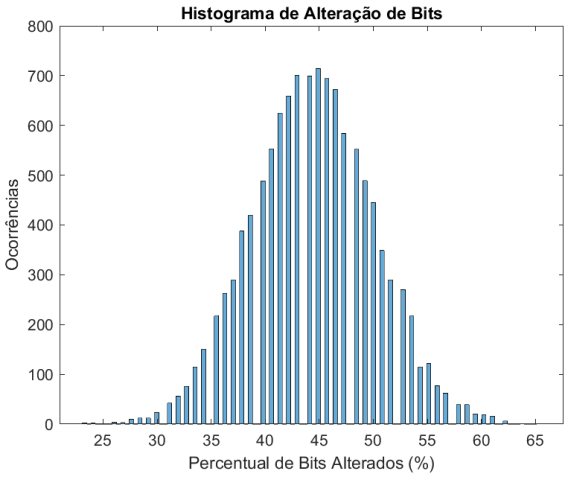

Figura 12 – Histograma para 2 rodadas

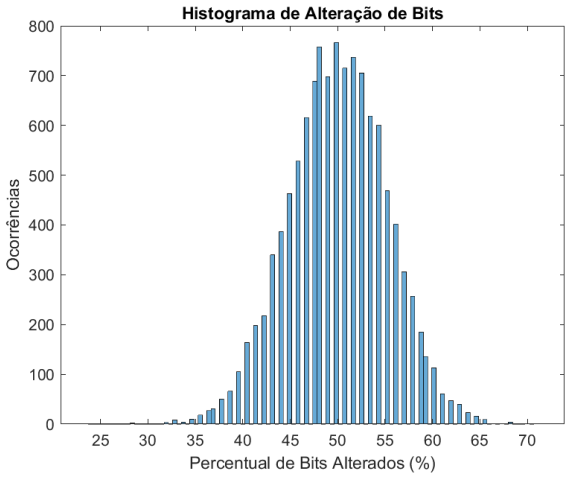

Figura 13 – Histograma para 3 rodadas

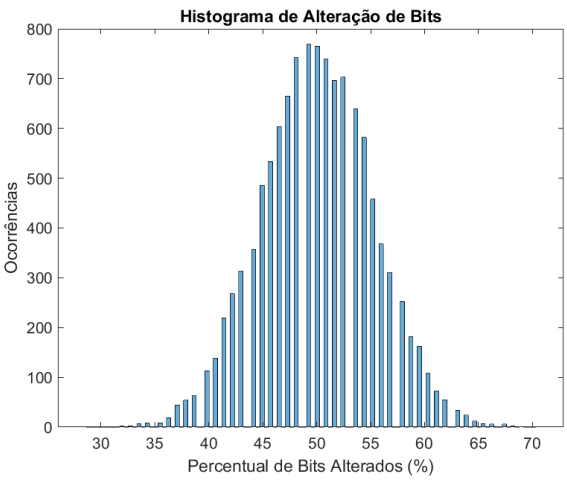

Figura 14 – Histograma para 4 rodadas

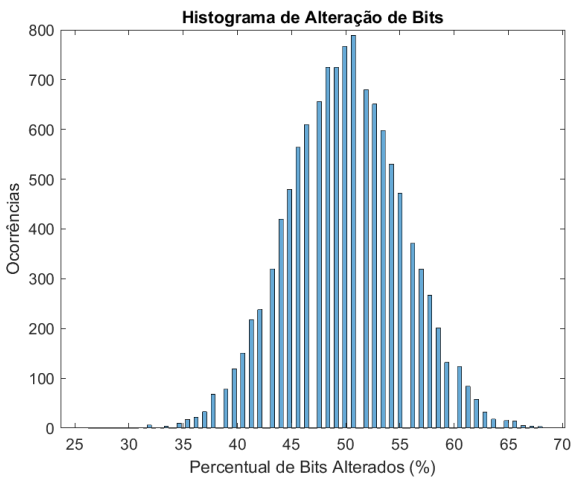

Figura 15 – Histograma para 5 rodadas

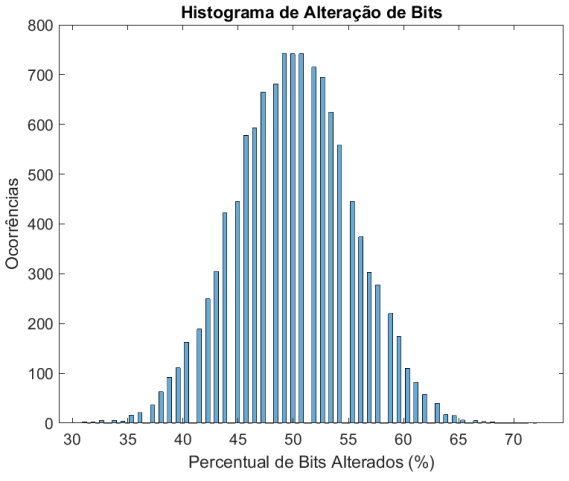

Figura 16 – Histograma para 6 rodadas

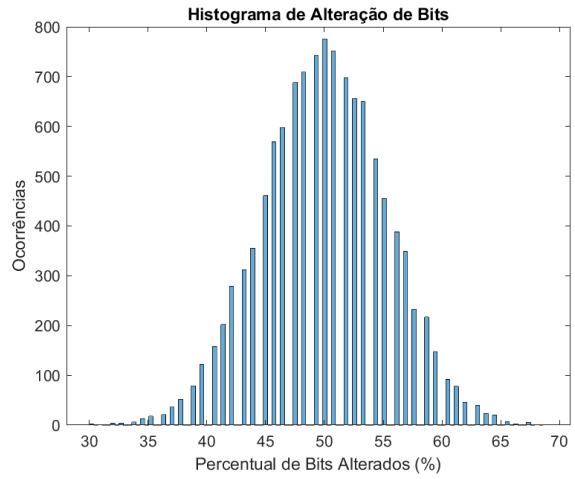

Figura 17 – Histograma para 7 rodadas

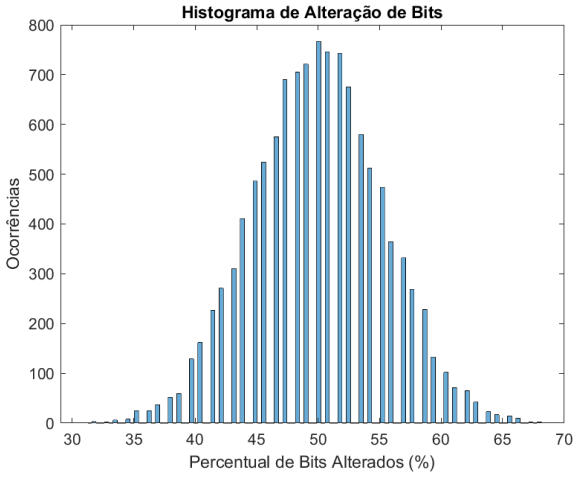

Figura 18 – Histograma para 8 rodadas

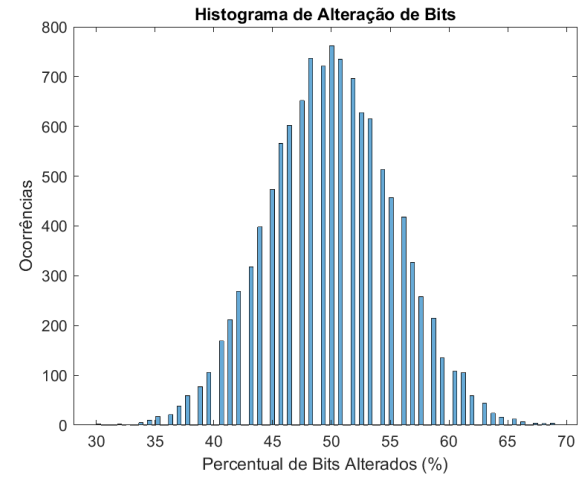

Figura 19 - Histograma para 9 rodadas

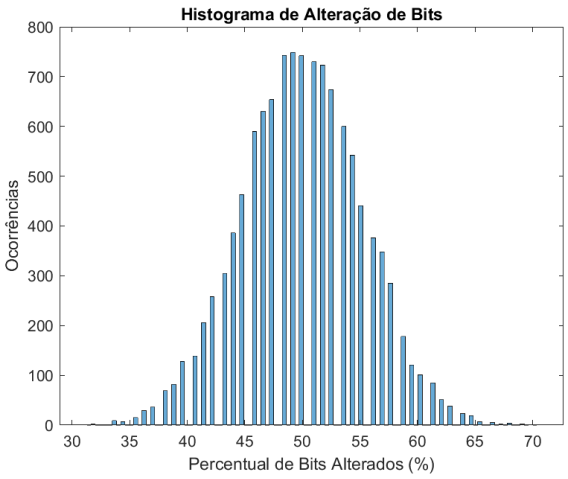

Figura 20 – Histograma para 10 rodadas

Com os histogramas obtidos, é possível perceber que a partir de três rodadas a média de bits alterados é de aproximadamente de 50%. Portanto, a partir de três rodadas

podemos considerar que a rede teve um bom desempenho. O bom desempenho é considerado pois garantimos que pelo menos metades dos bits foram alterados, ao trocar somente um bit da mensagem. Assim podemos afirmar que para blocos de mensagens parecidos, o bloco cifrado não vai ser semelhante. A média percentual da alteração dos bits pode ser observada na Figura 21.

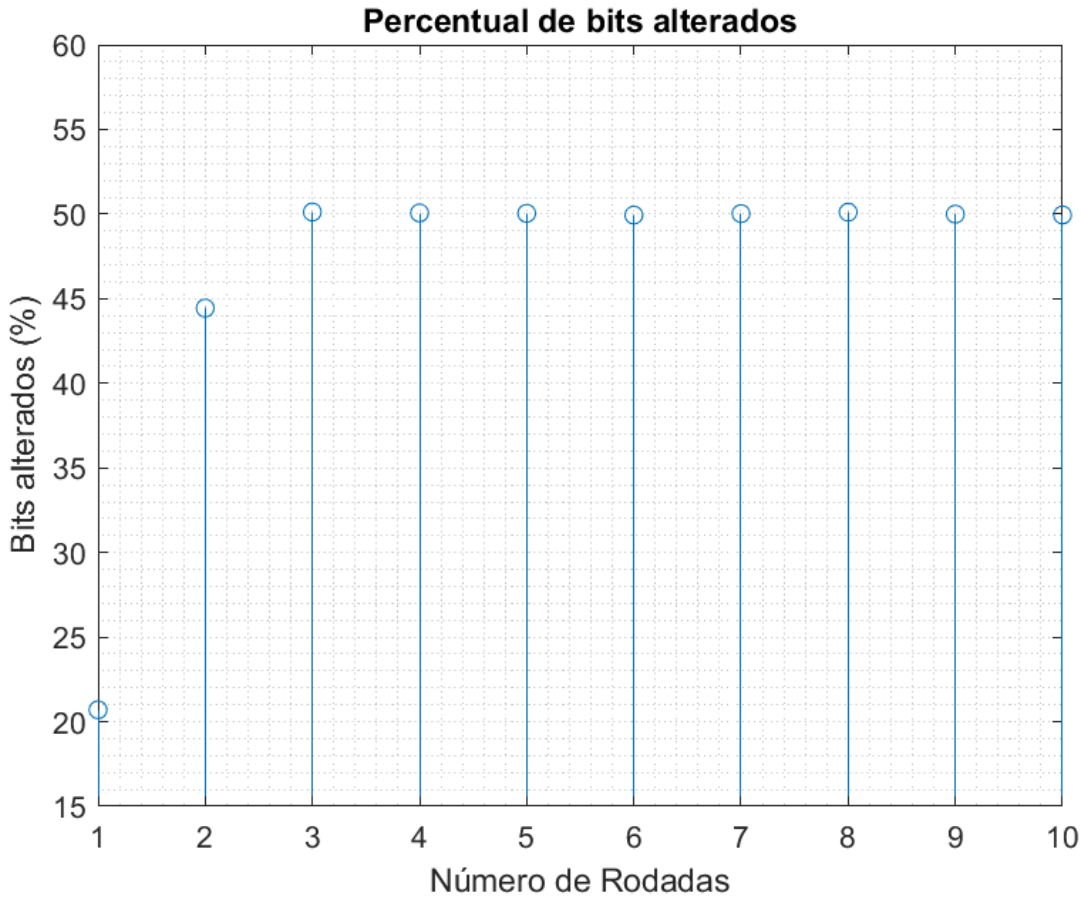

Figura 21 – Percentual de bits alterados

3.4 – Análise da Confusão

O processo para a análise da confusão é bastante semelhante ao da difusão com o mesmo número amostras, mas com 13 rodadas, conforme abordado na Seção 3.3. Fixando as chaves e o bloco da mensagem, é realizada a operação na rede de Feistel. O bloco criptografado é guardado, posteriormente são gerados outros blocos para comparação. Os blocos para comparação são gerados agora alterando a chave, ou seja o bloco da mensagem não vai ser alterado. A análise da Seção 3.2 foi feita alterando um bit da mensagem, mas para chave é necessário haver uma conversão. A conversão ocorre pelo fato do vetor de chave não ser bits, e sim valores de fase.

Foi criada uma tabela de conversão para as fases em bits, conforme mostrado na Tabela 1. Especificando um comprimento de dez bits para a chave, foi especificado um valor binário para cada valor de fase.

Tabela 1 – Conversão de Fase para Binário

Fase (rad)	Valor Binário
0,00000	0000000000
0,00613	0000000001
0,01226	0000000010
0,01839	0000000011
:	:
:	:
:	:
6,27705	1111111110
2π	1111111111

Com a Tabela 1, foi selecionada uma das chaves para a conversão. No caso, a partir do vetor de chaves da fase, foi selecionado cada posição e convertido em binário. Exemplificando, se a fase da primeira posição for 0,00613 rad, ela será transformada em 0000000001. Isso foi realizado para todas as 64 fases do vetor da chave, totalizando ao final 640 bits. A partir do vetor binário de 640 bits, realizou-se a análise da confusão, variando um bit de cada posição desse vetor. O procedimento foi alterar um bit por vez, e com o auxílio da tabela, converter o vetor alterado em fases. Para o exemplo citado, se os bits da chave forem 0000000001, alterando um bit temos: 0000000011. Ao converter novamente para fases, temos que na posição onde a fase era 0,00613 rad, agora será de 0,01839 rad.

A cada bit trocado, foi realizada a operação com a rede de Feistel e salvo o novo bloco encriptado. Após variar todos os bits da mensagem, foi comparado quantos bits foram alterados dos blocos cifrados encontrados com o bloco original. Portanto, a diferença para o procedimento da Seção 3.2 é que ao invés variar os bits da mensagem, foi variado os bits da chave. Esse procedimento foi realizado para diferentes valores de rodadas e construídos seus respectivos histogramas, conforme as Figuras 22 a 34. Os histogramas mostram a quantidade de vezes que ocorreu cada valor percentual.

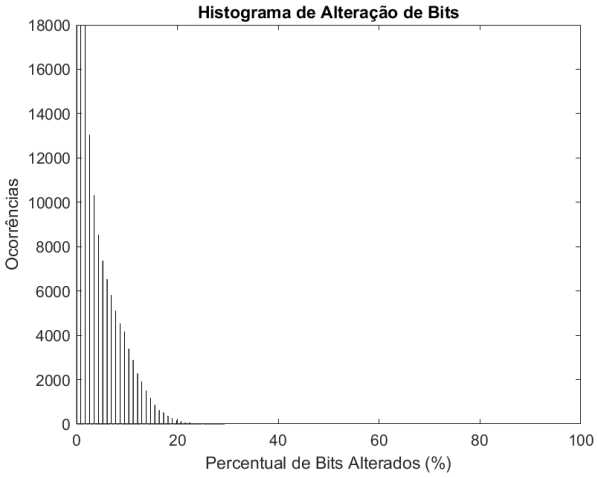

Figura 22 – Histograma para 1 rodada

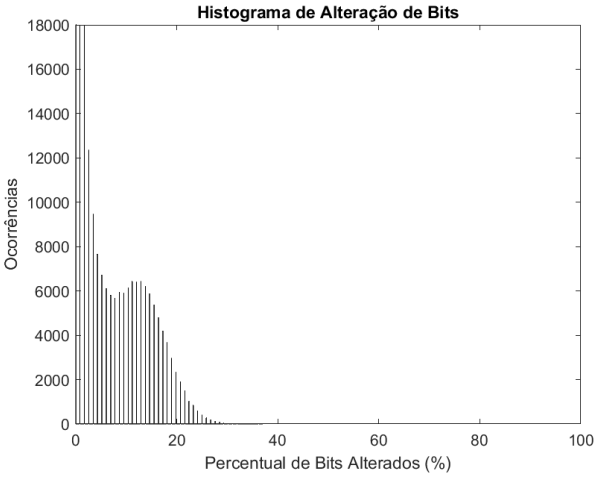

Figura 23 – Histograma para 2 rodadas

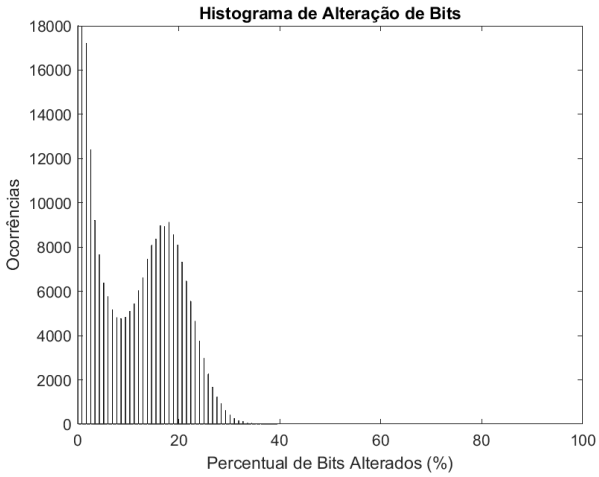

Figura 24 – Histograma para 3 rodadas

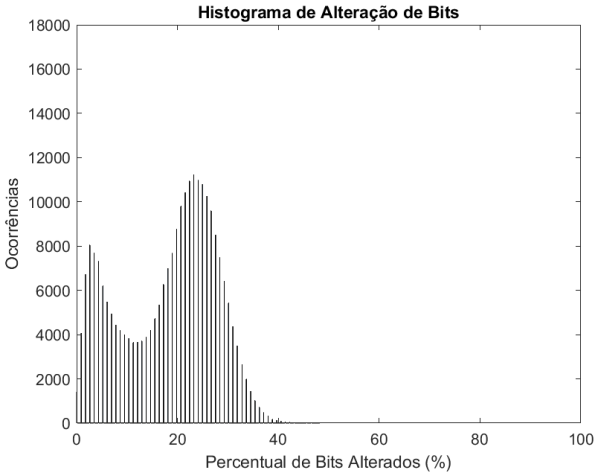

Figura 25 – Histograma para 4 rodadas

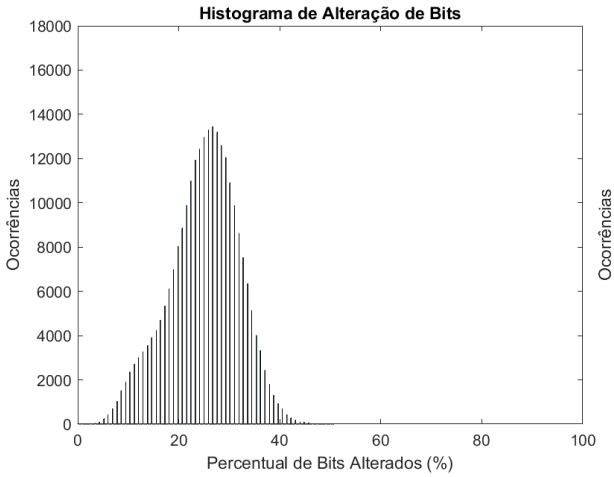

Figura 26 – Histograma para 5 rodadas

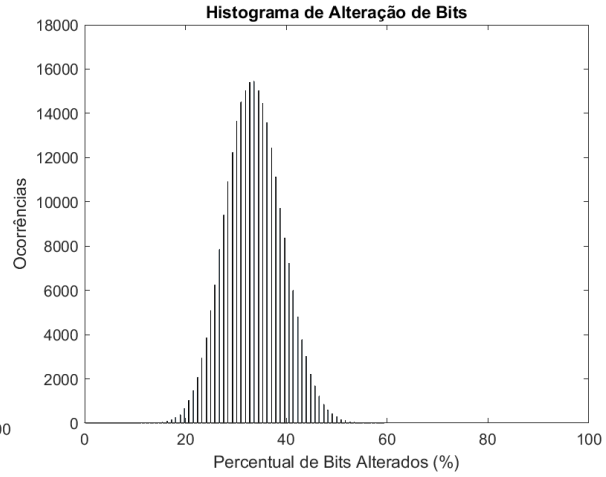

Figura 27 – Histograma para 6 rodadas

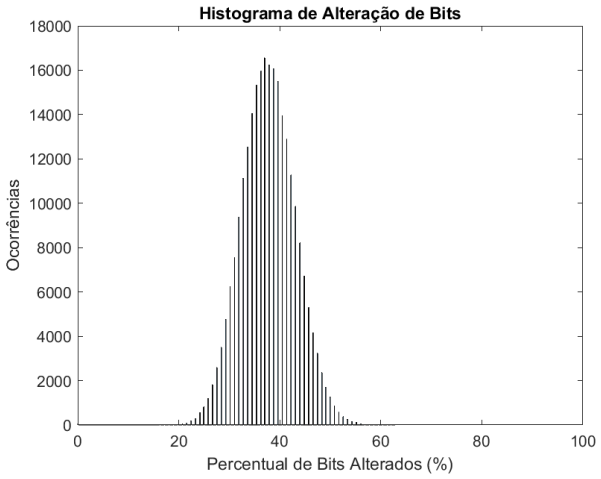

Figura 28 – Histograma para 7 rodadas

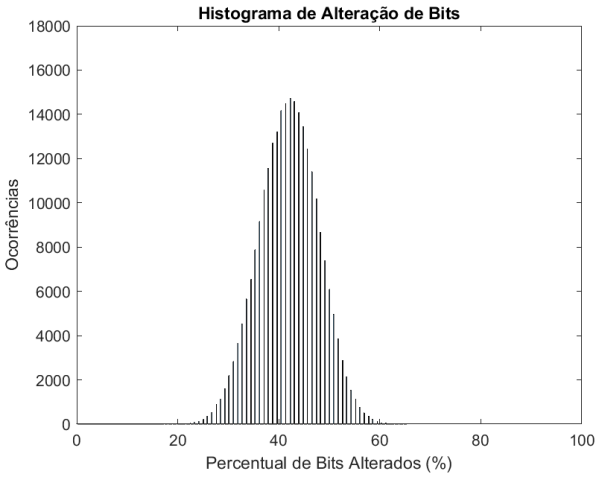

Figura 29 – Histograma para 8 rodadas

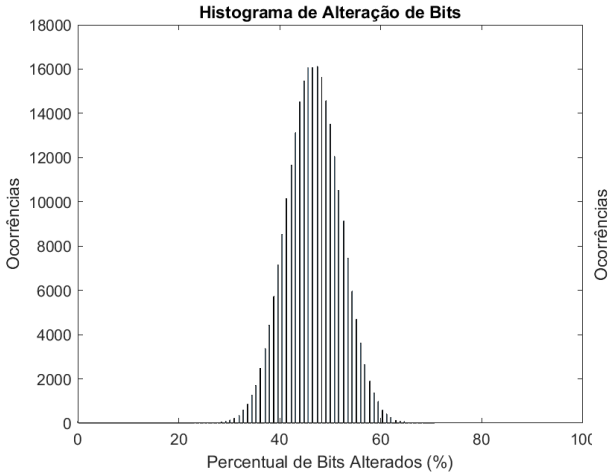

Figura 30 – Histograma para 9 rodadas

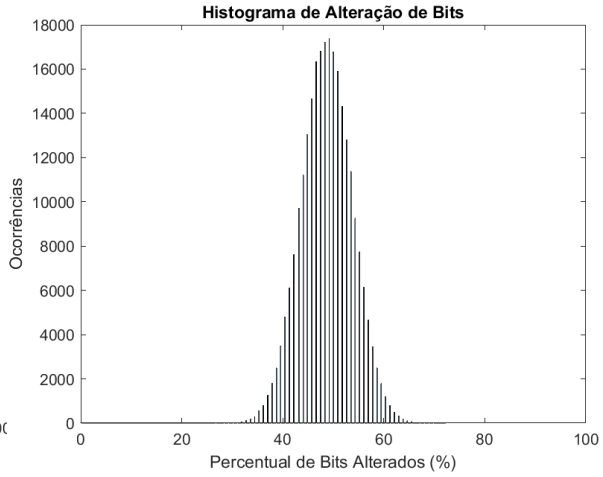

Figura 31 – Histograma para 10 rodadas

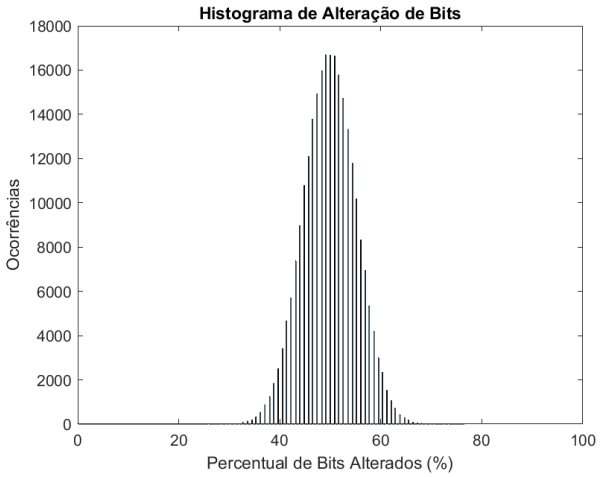

Figura 32 – Histograma para 11 rodadas

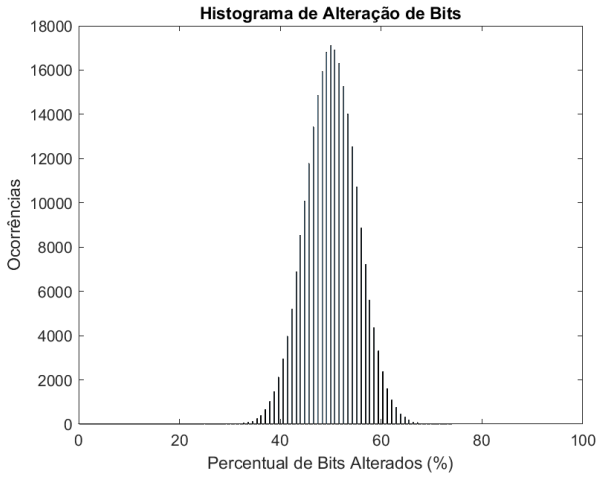

Figura 33 – Histograma para 12 rodadas

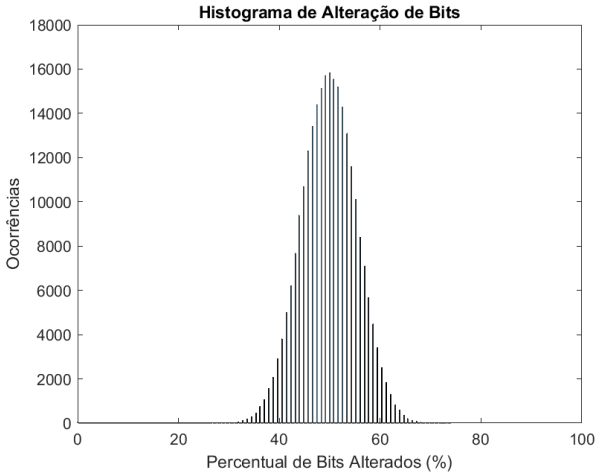

Figura 34 – Histograma para 13 rodadas

Com os valores dos histogramas, foi gerada a Figura 35 da média de bits alterados de cada um. Com o uso da figura das médias, é possível observar que a partir de onze rodadas temos uma média de pelo menos 50% dos bits alterados. Assim, a partir desse valor o desempenho da confusão é bom, pelo mesmo critério utilizado na Seção 3.2. Portanto, temos que depois de onze rodadas ou mais, chaves muito parecidas alteram pelo menos a metade dos bits na codificação de um mesmo bloco.

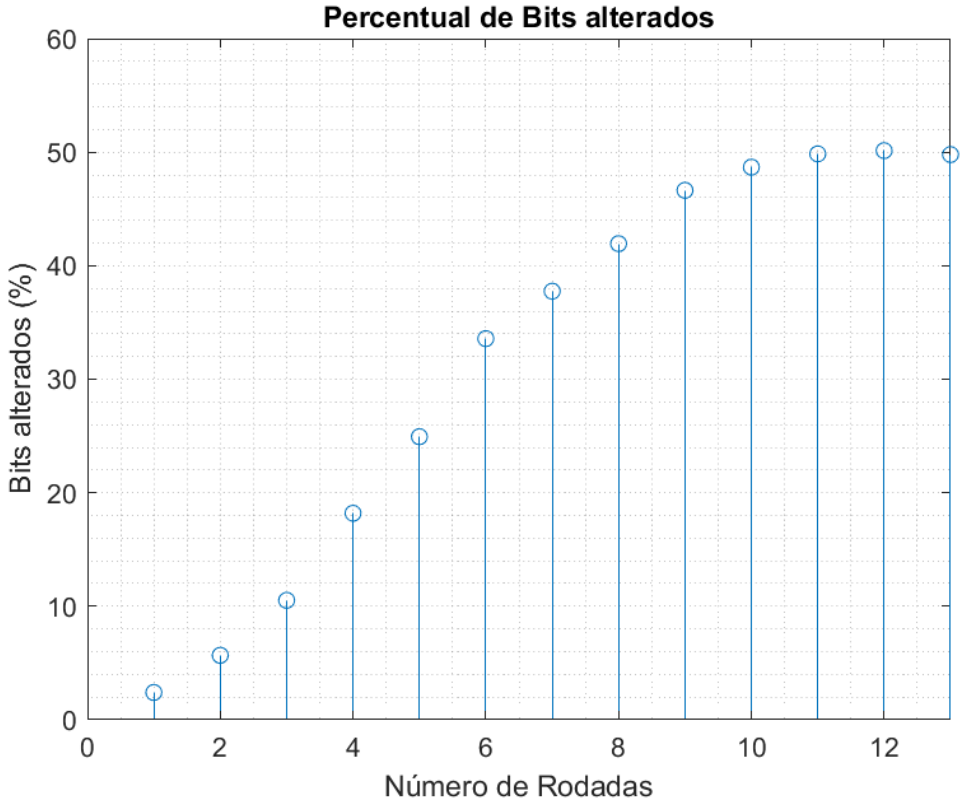

Figura 35 – Percentual de bits alterados

Comparando com a difusão, para se obter um valor de 50% dos bits alterados, foi necessário um maior número de rodadas. Isso ocorreu devido ao fator de que ao variar um bit na chave, a alteração de fase dependendo da posição do bit é pouco significativa. Ao analisar a tabela 1 é possível perceber que dependendo do bit alterado, a variação de fase é de apenas 0,00613 rad. Esse valor representa uma alteração de apenas 0,1% aproximadamente de todos os valores de fase que a chave pode ter. Diferentemente da difusão onde ao variar um bit 1 para 0 e alterava completamente o valor da posição, na confusão é apenas o pequeno valor percentual citado acima. Pelo motivo da variação de fase ser pouco significativa ao trocar o bit, foi necessário um maior número de rodadas na confusão.

Nos histogramas para valores baixos de rodadas, observa-se que o formato do histograma não corresponde à uma forma gaussiana como para os outros valores. Esse fato ocorre devido à proximidade com o eixo nulo, onde a curva é limitada ao valor mínimo. A limitação ocorre pois não é possível existir uma variação negativa dos bits, tornando as curvas próximas a zero não lineares. Pelo fato das curvas para valores baixos de rodada não serem lineares, elas não apresentam uma aparência gaussiana no histograma.

3.5 – Considerações

Durante esse capítulo foram abordados os resultados obtidos nas simulações, e apresentadas algumas considerações sobre os mesmos. Foi possível observar que, a partir de três rodadas a rede apresentou um bom desempenho de difusão. Para a difusão, o bom desempenho foi a partir de onze rodadas. Portanto, em uma rede de Feistel aplicada a sinais, temos confusão e difusão ocorrendo a partir de onze rodadas. Com o comportamento encontrado, observa-se que as rede de Feistel aplicadas a sinais são promissoras para aplicações práticas.

4 – Conclusões

Este trabalho consistiu em avaliar a BER, a difusão e a confusão de uma rede de Feistel aplicada a criptografia de sinais. Para a realização do trabalho foi necessário a utilização de códigos no *software* Matlab. Esses códigos foram implantados por [Bragagnolle, 2018]. Foi utilizada para a simulação um sinal equivalente complexo em banda base de um sinal QPSK.

Os resultados indicam que uma única rodada da rede de Feistel é suficiente para produzir um sinal encriptado com uma BER de 50% como desejado. Três rodadas da rede de Feistel são suficientes para obter uma difusão média de 50%, e para a confusão foram necessárias onze rodadas para atingir 50%. A quantidade maior de rodadas do que a difusão é justificada pois, a variação de um bit nos bits menos significativos da chave representam uma alteração muito pequena das fases da chave que encriptou o sinal.

Os resultados obtidos sugerem que a rede de Feistel aplicada à sinais pode ser utilizada em aplicações práticas. Uma continuidade do trabalho teria pelo menos dois pontos importante para serem executados. O primeiro ponto é referente a questão de desempenho criptográfico, onde seria analisado a robustez da técnica à outros tipos de ataque como: Ataques de força bruta, ataques de criptoanálise diferencial e ataques de criptoanálise linear. Além disso, também é importante avaliar a questão de segurança semântica como está sendo estudado em [Souza, 2019]. Outro ponto, é referente a implementação pratica do trabalho, implantando a técnica em FPGA ou em USRP. A implementação prática era o objetivo inicial deste trabalho, mas não pode ser concretizada de maneira experimental por conta da pandemia.

REFERÊNCIAS

Julio, R. A. “DADOS SÃO O NOVO PETRÓLEO, DIZ CEO DA MASTERCARD – EXCETO POR UM PEQUENO DETALHE”, Época negócios, 2019. Disponível em: <https://epocanegocios.globo.com/Empresa/noticia/2019/07/dados-sao-o-novo-petroleo-diz-ceo-da-mastercard.html>. Acesso em: 20 de Outubro de 2020.

Stallings, W. “CRIPTOGRAFIA E SEGURANÇA DE REDES, PRINCÍPIOS E PRÁTICAS”. 6° Ed. Pearson, 2014.

Terrada. R. “SEGURANÇA DE DADOS: CRIPTOGRAFIA EM REDE DE COMPUTADOR”. Editora Blucher, 2008.

Burnett, S.; Paine, S. “CRIPTOGRAFIA E SEGURANÇA: O GUIA OFICIAL RSA”. Gulf Professional Publishing, 2002.

Katz, J.; Lindell Y. “INTRODUCTION TO MODERN CRYPTOGRAPHY”, 2° Ed., CRC Press, 2015.

Shannon, C. E.; Weaver, W. “THE MATHEMATICAL THEORY OF COMMUNICATION”. University of Illinois Press, 1949.

Tanembaum, A. S. “REDES DE COMPUTADORES”, 5°Ed., Pearson, 2013

Abbade, M. L. F.; Lessa, L. S.; Santos, M. de O.; Prado, A. J. do; Aldaya, I. “A NEWDSP-BASED PHYSICAL LAYER ENCRYPTION TECHNIQUE APPLIED TO PASSIVE OPTICAL NETWORKS” 20th International Conference on Transparent Optical Networks (ICTON), 2018.

Breed, G. “BIT ERROR RATE:FUNDAMENTAL CONCEPTSAND MEASUREMENT ISSUES”. High Frequency Electronics, Summit Technical Media, LLC, January 2003.

Bragagnolle, T. A. “SEGURANÇA DE CAMADA FÍSICA APLICADA A REDES ÓPTICAS”. Dissertação (Mestrado em Engenharia Elétrica- Sorocaba/ São João da Boa Vista) - Universidade Estadual Paulista Júlio de Mesquita Filho. Início: 2018.

Souza, W. S. “ADAPTAÇÃO DE CRIPTOGRAFIA ESPECTRAL AO PARADIGMA DO ADVANCED ENCRYPTION STANDARD”. Dissertação (Mestrado em Engenharia Elétrica- Sorocaba/ São João da Boa Vista) - Universidade Estadual Paulista Júlio de Mesquita Filho, Fundação de Amparo à Pesquisa do Estado de São Paulo. Início: 2019.

Feistel, H.; Notz, W. e Smith, J. “SOME CRYPTOGRAPHIC TECHNIQUES FOR MACHINE-TO-MACHINE DATA COMMUNICATIONS”. Proceedings of the IEEE, 1975.

Bragagnolle, T. A. “EXAME DE QUALIFICAÇÃO: REDE DE FEISTEL ADAPTADA À CRIPTOGRAFIA DE SINAIS”, Programa de Pós-Graduação em Engenharia Elétrica, UNESP - São João da Boa Vista, 2020.